US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/29/2022

OPDIV:

ACF

Name:

OCSE Data Center

PIA Unique Identifier:

P-6810356-560881

The subject of this PIA is which of the following?

General Support System (GSS)

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?

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.

Three new minor applications/functions have been added to the Office of Child Support Enforcement (OCSE) Data Center General Support System (ODC GSS). The ODC GSS now hosts a public facing website called Child Support Collaboration and a batch application called Electronic National Medical Support Notice (e-NMSN). The ODC GSS also hosts a new Central Authority Payment (CAP) minor application.

Describe the purpose of the system.

The ODC GSS is a secure gateway for the Office of Child Support Enforcement's (OCSE's) internal and external stakeholders to access tools and services that support the OCSE mission. This system is housed in a FedRamp approved cloud platform.

The ODC GSS hosts Batch Services, which is a minor application that provides a system-based method for authorized parties to securely send and retrieve information between state child support

enforcement agencies and external child support program partners, such as employers, Health Plan Administrators (HPA), Financial Institutions (FI), or Foreign Authorities (FA) which serve as central authorities in foreign treaty countries or foreign countries that are the subject of a declaration under 42 U.S.C. 659a. These batch applications include:

The electronic income withholding order (e-IWO) minor application, which consists of various batch programs that support the electronic transmission of income withholding order data between states and employers.

The Federally Assisted State Transmitted (FAST) Levy minor application that allows states and FIs to exchange lien/levy information for matches identified by the FI performing the data match. The FAST Levy process also enables a state to send a lien/levy request to an FI and receive an acknowledgment through a batch process.

The e-NMSN minor application that assists states and employers in providing an electronic mechanism for exchanging medical support notice information. The e-NMSN process exchanges Part A and Part B of the NMSN forms electronically between stakeholders.

The Central Authority Payment (CAP) minor application, which maintains information to support the exchange of child support disbursements transmitted from states to a FA.

The ODC GSS houses the Child Support Collaboration application and hosts the Child Support Portal (CSP). The OCSE Collaboration application is a common gateway that allows users to document and collaborate on established topics supporting the OCSE mission. No PII is maintained for this application.

The CSP, a major application that provides access to ODC GSS tools and services, is covered under a separate Privacy Impact Assessment (PIA) specific to that system.

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

The ODC GSS hosts Batch Services minor application, which process file exchanges between various stakeholders, including external partners – such as employers and financial institutions.

The ODC GSS hosts four other minor batch applications which are the e-IWO, the e-NMSN, the FAST Levy, and the CAP minor application. The following information related to batch-parent registration for these applications is collected, maintained, and stored within the ODC GSS:
Business name
Business contact information (phone and email address)
Federal Employer Identification Number (FEIN)
Server credentials
Internet Protocol (IP) address/Device Identifiers
e-IWO data includes information found on the state's income withholding order and the employer's acknowledgment, including individuals' date(s) of birth.

FAST Levy data includes obligor's financial information.
e-NMSN files contain a Part A and Part B form with employment information, child support case information, medical records number, and health care coverage information. E-NMSN maintains information about health insurance information, and information about parents and children, including child(ren)'s gender and date(s) of birth.

CAP program data includes: obligor names and social security numbers; FA name, FIPS code and FA child support case identifier; U.S. state name and state case number; amount and date of

payment; medical support indicator; and employment termination indicator.

The external partners will provide information to and receive information from the system but will not have access to the information within the system.

OCSE will maintain the records, receiving them from one stakeholder and transmitting them to another, but will not use the information for its own purposes.

The ODC GSS also houses a web-based minor application, the OCSE Collaboration web application. The following information is collected, stored, and maintained to support application registration:
Full names
Phone numbers and emails
Employer name and address
Answers to three of the following security challenge questions: pet's name, make/model of first car, and city of the user's first job, childhood nickname, oldest cousin's first name, location of nearest sibling, town of first job, school name attended in sixth grade, city where they met their spouse, name of childhood best friend, name of favorite historical person, name of favorite author, first name of prom date.

OCSE Collaboration allows federal worker users to upload files relating to their tasks, workflow, events, and calendars. No PII is contained in this application.

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

The system will be used to facilitate electronic exchanges of information about individual participants in child support cases, between state child support enforcement agencies and other external partners such as employers, HPAs, FIs, and FAs. The child support enforcement agencies and other external partners will use the gateway system to electronically submit information to and receive information from each other, through OCSE.

Multiple child support program partners will utilize the gateway system to electronically send and receive information:
State child support enforcement agencies will use the system to transmit e-IWOs to employers and e-NMSNs to employers and HPAs. State child support enforcement agencies will also use the system to create levy actions for distribution to multiple FIs, and to initiate child support disbursements to FAs through the CAP program.
Employers will use the system to respond to state child support enforcement agencies regarding e-IWOs and to provide information about terminations and health insurance coverage provided by the employer. Employers and HPAs will use the system to respond to state child support enforcement agencies regarding e-NMSNs.
FIs will use the system to receive and respond to levy actions from multiple state child support enforcement agencies.
FAs will use the system to receive information about child support disbursements from U.S. states.

Access to any batch services is controlled by network and system-based access controls on the infrastructure. All e-IWO, FAST Levy, e-NMSN Part A and Part B, and CAP transferred files are passed through data and backup copies which are stored no more than 60 days as per data retention policy.

Batch partner contact information is kept indefinitely in the ODC GSS database until no longer needed.

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

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Financial Accounts Info

Device Identifiers

Employment Status

Federal Employee Identification Number (FEIN), Sex, Gender

Batch Partner's server user name and password

E-IWO/FAST Levy child support case data and case ID; Case Type (title IV-D or non IV-D), State American National Standards Institute (ANSI) code, state ANSI county code, state case identification number, state member identification number
Participant Type (custodial, noncustodial, putative father, child); Family Violence indicator (domestic or child abuse)
NMSN Part A and Part B

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

Public Citizens

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

Foreign Authority business contacts

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of the batch services PII is to register the business within the system to facilitate data sharing. The primary purpose of the e-IWO, FAST Levy and e-NMSN program PII is to ensure accurate data reporting to the employer or FI to facilitate child support actions against the correct individual. The primary purpose of the CAP program PII is to ensure the proper identification of an international child support payment and its disbursement to the correct FA.

The primary purpose of Collaboration application PII is to register users for a system account.

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

There are no secondary uses for either group of PII.

Describe the function of the SSN.

Primary Subject identifier

Cite the legal authority to use the SSN.

42 U.S.C. § 652(a)(7) and (9), Duties of Secretary 42 U.S.C. § 653(a)(1), Federal Parent Locator Service42 U.S.C. § 666, Requirement of statutorily prescribed procedures to improve effectiveness of child support enforcement

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

Article 6 of the Hague Convention on the International Recovery of Child Support and Other Forms of Family Maintenance (November 23, 2007)
42 U.S.C. § 652, Duties of Secretary
42 U.S.C. § 654, State plan for child and spousal support
42 U.S.C. § 654a, Automated data processing
42 U.S.C. § 654b, Collection and disbursement of support payments
42 U.S.C. § 659, Consent by the United States to income withholding, garnishment, and similar proceedings for enforcement of child support and alimony obligations
42 U.S.C. § 659a, International support enforcement
42 U.S.C. § 666, Requirement of statutorily prescribed procedures to improve effectiveness of child support enforcement
42 U.S.C. § 666a, Requirement of statutorily prescribed procedures to improve effectiveness of child support enforcement
Otherwise, there is no disclosure of the data unless there is need for an investigation of an incident related to a breach.

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.

OCSE Data Center General Support System, HHS/ACF/OCSE, 09-80-0389, December 21, 2021 (86

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

State/Local/Tribal

Foreign

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable – an OMB Information collection approval number is not needed for the ODC GSS.

Is the PII shared with other organizations?

Yes

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

Other Federal Agencies

FAs will receive information about child support disbursements from U.S. states.

State or Local Agencies

The ODC GSS shares responses from Employers, HPAs, and FIs to provide states with acknowledgments to requests for income withholding or medical support enrollment.

Private Sector

The ODC GSS shares income withholding orders and national medical notices from states to provide Employers, HPAs and FIs instructions to withhold income or enroll children in health care plans for child support compliance purposes.

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. OCSE does not have Information Sharing Agreements (ISAs) with FAs participating in the CAP program. Instead, sharing and disclosures are covered under the Hague Convention on the International Recovery of Child Support and Other Forms of Family Maintenance.

Describe the procedures for accounting for disclosures.

Employer, HPA, and FI profiles kept at the ODC GSS are not shared or disclosed. The e-IWO, FAST Levy, e-NMSN, and CAP file transfers are tracked in audit records which are stored in the ODC GSS database. Registration for the Collaboration application is voluntary. Users must opt-in and must register a profile to gain access.

Audit logs capture all administrator activities. All file transfer details are tracked in audit logs. Logs from the ODC are sent to a Security Information and Event Management (SIEM) tool for automated alerting of unauthorized activity.

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 PII collected for employer, HPA, FI, and Collaboration users is voluntary, and notice of the collection occurs at the time of account registration. If an employer, HPA, FI, or Collaboration user chooses to not provide the PII, then a system account will not be created, and that organization will not receive any data.

The PII collected as part of the e-IWO, e-NMSN, FAST Levy, and CAP records is mandated by federal statute and does not require prior notice. Data use is published in the OCSE Data Center General Support System, System of Records Notice, in the Federal Register at 86 FR 72245 on December 21, 2021.

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.

Since the PII for batch partner registration is collected voluntarily, organizations can elect to not register for batch file transfers. However, by choosing to not provide their PII, the organization will not be granted a batch connection.

There is no opt-out process for individual PII that is collected as part of an e-IWO, e-NMSN, FAST Levy, or CAP record as this information is mandated by federal statute.

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

Individual PII that is part of an e-IWO, e-NMSN, FAST Levy, or CAP record is not taken into account for notification prior to any major changes to the system as the collection is mandated by federal statute.

Email notifications are sent to registered organizations and batch partners to notify them of upcoming major changes and the impact of those changes.

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 acting as points of contact for businesses and FIs may contact the ODC GSS system administrators to correct contact information stored at the ODC GSS. The ODC GSS contact information is provided by HHS on the eIWO website. Alternatively, direct contact information for ODC GSS system administrators is provided to the organization during the batch registration process.

For eIWO and FAST Levy PII, no process is in place because the information is collected at the state level and then fed up to the ODC GSS. If an individual had a concern about their PII then it would have to be resolved at the collection point, in this case the state.

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

For batch partner contact PII, a process is partially in place. The ODC GSS ensures integrity and availability through its security controls. For email addresses, an automated process ensures accuracy and relevancy by "bouncing back" emails when a partner's address is no longer valid. ODC GSS personnel contact the partners with invalid email addresses to update their contact information. A process is in development for the rest of the batch partner contact information PII.

For e-IWO, FAST Levy, e-NMSN, and CAP PII, no process is in place because the information is collected at the state level, and from external partners, and then fed up to the ODC GSS. The ODC GSS is a pass-through facility, so states must ensure the integrity, availability, accuracy and relevancy of this PII.

For Collaboration application users, no process is in place. Users must maintain the accuracy of their profile information. The ODC GSS ensures integrity and availability.

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

Administrators:

System administrators have access to all PII within the ODC GSS to include the files the help desk staff assist with and additionally, the PII associated with the batch partner records. System administrators can also help troubleshoot problems that the help desk staff are unable to resolve prior to providing a temporary solution and receive email alerts associated with the ODC GSS.

Contractors:

Direct contractors make up the pool of system administrators and help desk staff.

Others:

The Help Desk has access to PII to assist file transfer partners when there are problems with batch file transfer processes such as: data validation errors, connection errors, and other problems that prevent successful file transfers. The Help Desk also provides temporary solutions such as transmitting files using OCSE-approved methods listed in the OCSE sensitive data handling procedures for PII.

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

Only ODC GSS system administrators have access to batch partner profiles and transfer files for e-IWO, FAST Levy, e-NMSN, and CAP. System administrators receive access to the system based on business need and manager approval. Federal management must approve all access for administrators, developers, and contractors.

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.

There is only one group of individuals with access to PII in the ODC GSS and those individuals are categorized as system administrators. The methods used to limit access to the amount of PII a system admin can access at a given time include Lightweight Directory Access Protocol (LDAP) and Secure Shell (SSH) server configurations.

Collaboration application users may only access their own profile information. Collaboration application administrators may access their own profile as well as all other user profiles to perform their duties.

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 and annual security awareness training is required for all. Security awareness and role-based training is provided by Health and Human Services (HHS), Administration for Children and Families (ACF), and OCSE.

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

Additional annual training includes the review of Internal Revenue Service (IRS) regulations, federal statutes, HHS and ACF regulations, and refresher material. OCSE provides additional training based

on employee role and job function within the operating division (OpDiv) on an annual basis - this includes:
HHS Information Security for Managers (given to all project managers and task leads)
HHS Information Security for Information Technology Administrators (given to remaining project staff in non-management or IT positions)
Role-based security training is required for employees with elevated privileges.

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.

The minimum retention period for system data (to include organization profile PII) within the ODC GSS, as defined in the SORN, is 5 years. Since the ODC GSS processes federal tax information (FTI) for the CSP, audit data must be retained for 7 years to comply with IRS safeguard requirements as specified in IRS Publication 1075. Currently, file transfer logs are kept for 180 days.

A backup copy of each file transferred for e-IWO, FAST Levy, e-NMSN, and CAP is retained for 60 days in accordance with the SORN. A script runs daily which checks each backup file on the file system and deletes files older than 60 days.

Upon approval of a disposition schedule by the National Archives and Records Administration (NARA), the records will be deleted when eligible for destruction under the schedule, if the records are no longer needed for administrative, audit, legal, or operational purposes. ACF anticipates requesting NARA’s approval of retention periods of approximately 60 days for the information contained in the transmission files (i.e., long enough to confirm receipt or to resend if necessary), up to 120 days to correct errors, up to one year to reconcile information with external partners, and up to seven years for the audit log records. Approved disposal methods for electronic records and media include overwriting, degaussing, erasing, disintegration, pulverization, burning, melting, incineration, shredding, or sanding.

The minimum retention period for all Collaboration data is 5 years. Cutoff for Collaboration user profiles is defined as the date in which the account is deactivated.

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 National Institue of Standards and Technology (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.

Note: web address is a hyperlink.

Session Cookies that do not collect PII.