

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

08/11/2025

**OPDIV:**

ACF

**Name:**

Debtor File

**PIA Unique Identifier:**

P-7284550-654452

**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?**

No

**Identify the operator.**

Agency

**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

Significant System Management Change

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

The system is migrating to the Amazon Web Services (AWS) cloud. No other significant changes have been made to the system since the last Privacy Impact Assessment (PIA) approval.

**Describe the purpose of the system.**

The Debtor File (DF) is a data repository containing individuals' past-due child support debt information, submitted by state and tribal Title IV-D agencies (IV-D agencies) to the Office of Child Support Services (OCSS). Its primary purpose is to improve the ability of IV-D agencies to collect past-due child support. This data repository is used to provide information to the following: Department of Treasury for Federal Income Tax Refund Offset and Administrative Offset programs, to Department of State for the Passport Denial program, to multi-state financial institutions for matching against financial accounts, to insurance providers for matching against insurance claim information, and to federal agencies to determine eligibility of individuals applying for any federal

loan (other than a disaster loan), loan guarantee, or loan insurance. The DF consists of three minor applications: Federal Offset (tax and administrative offset and passport denial), Multi-state Financial Institution Data Match (MSFIDM) and Insurance Match, which are covered under this PIA.

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

The DF system collects information from IV-D agencies regarding past-due child support owed by noncustodial parents, and includes: the parents' Personally Identifiable Information (PII), such as: name, Social Security Number (SSN), date of birth, place of birth, mailing address, and Taxpayer Identification Number (TIN); the amount of past-due child support owed by the individual, adjustments to such amount, information on each enforcement remedy applicable to the individual as reported by IV-D agencies, the amount of past-due support collected as a result of offset collections, and a history of updates by the IV-D agency to the records.

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

The information DF collects from IV-D agencies is compared against information pertaining to federal tax refunds, federal administrative payments, and U.S. passports. The DF information is also compared with information maintained by insurers (or their agents) and State Workers' Compensation agencies regarding insurance claims, settlements, awards, and payments. The information resulting from these information comparisons provides asset information to IV-D agencies for the collection of past-due child support. The collection of this data is mandatory. Federal law requires the collection of this information for the administration of the child support program and for other authorized purposes.

Federal assistance and lending agencies also receive DF information through the U.S. Treasury's Do Not Pay system. DF information is used by these agencies to determine eligibility of individuals applying for any federal loan (other than a disaster loan), loan guarantee, or loan insurance when payments to such individuals are subject to administrative offset because of delinquent child support obligations.

**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  
Mailing Address  
Financial Accounts Info  
Taxpayer ID  
Child support arrearages and payment updates  
Place of birth

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

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

**How many individuals' PII is in the system?**

1,000,000 or more

**For what primary purpose is the PII used?**

The primary purpose of the PII is to improve the ability of IV-D agencies to collect past-due child support.

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

N/A

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

42 U.S.C. § 652(k), Duties of Secretary - Denial of passports for nonpayment of child support, § 652 (l), Facilitation of agreements between State agencies and financial institutions, and § 652(m), Comparisons with insurance information  
42 U.S.C. § 653(a)(2), Federal Parent Locator Service - Establishment; purpose, § 653(l), Restriction on disclosure and use, and § 653(m), Information integrity and security  
42 U.S.C. § 654(26), State plan for child and spousal support  
42 U.S.C. § 664, Collection of past-due support from Federal tax refunds  
Executive Order 13019, Supporting Families: Collecting Delinquent Child Support Obligations (September 28, 1996)

**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 Debtor File, HHS/ACF/OCSE, 09-80-0383, published in the Federal Register at 87 FR 3557

**Identify the sources of PII in the system.**

Government Sources  
State/Local/Tribal  
Other Federal Entities

**Identify the OMB Information collection approval number and expiration date**

Private Tax Offset, Administrative Offset, and Passport Denial Programs,  
OMB Control Number: 0970-0161, expires July 31, 2028.

**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.**

There are Memorandum of Understandings (MOUs) in place with the Department of Treasury, financial institutions, and security agreements with the states and tribes. Additionally, security agreements are in place with participating insurers.

**Describe the procedures for accounting for disclosures.**

Data is accessed by authorized case workers, and disclosures are tracked. Disclosures are only for agreed upon timeframes and purpose. Continuous review of agencies with disclosed information is done through audit log collection which provide the date and purpose of each disclosure to the IV-D agencies and also annually as part of an internal security inspection.

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

Prior notice is not given. Information collected is mandatory under federal statutes

**Is the submission of PII by individuals voluntary or mandatory?**

Mandatory

**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 option, as information collection is mandatory under federal statutes.

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

There is no process in place for notifying or obtaining consent from individuals whose PII is in the system when major changes occur to the system. Consent is not required because the information collected is mandated by federal statute. Please reference the OCSE Debtor File System of Records Notice (SORN) published in the Federal Register for more details.

**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.**

The DF system does not have a process in place for individuals to resolve concerns regarding inaccuracies in their PII. These concerns need to be addressed at the collection point, which in this case are the IV-D agencies.

If individuals believe that their information has been inappropriately obtained, used, or disclosed as a result of DF system activity, they may submit a notification directly to the Office of Child Support Services. The notification must specify what information was believed to have been obtained inappropriately.

Given there is no direct interaction with DF by the individuals whose information is maintained in the system, the individual would need to refer to the OCSE Debtor File SORN to obtain the address to which a request for records can be sent.

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

Data is reconciled with states and tribes annually and is continually updated and replaced. The reconciliation is performed using input files from the states and tribes pertaining to information about individuals owing past-due child support and information maintained by the Secretary of the Treasury concerning the following amounts payable to such individuals: refunds of federal income taxes; salary, wage, and retirement benefits; and income and benefits information. There are checks and balances from the federal to state and tribal level therefore, this process helps to improve the integrity, accuracy, and relevancy of the system data.

**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.**

Authorized users are the only ones allowed to access PII; administrators, developers, and contractors (not providing support to program initiatives) do not have access to PII.

**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 are in place which restrict users to the authorized data accesses.

**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 ACF Security and Privacy Compliance Awareness Training is required for all.

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

Annual training includes the review of Internal Revenue Service (IRS) regulations, federal statutes, HHS and ACF regulations, and refresher training. OCSS 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.**

Proposed DF records schedule (DAA-0292-2025-0005) has been submitted to ACF and is pending approval by NARA.

The proposed records retention schedule includes:

- (1) Master Files / Federal Offset Case Master (includes SSN, state, name, date of birth, case ID) – cut off at end of calendar year in which case is closed; delete 7 years after cutoff.
- (2) Master Files / Federal Offset Obligor and Address Master (includes SSN, name, state, sex) – cut off at end of calendar year in which case is closed; delete 7 years after cutoff.
- (3) Master Files / Multistate Financial Institution Data Match Person Archive Record (includes SSN) – cut off every 2 years; delete after cutoff.
- (4) Master Files / Insurance Match Activity File (includes SSN, case ID, name, date of birth, sex, phone, driver's license number, state, address) – cut off every 12 months; delete after cutoff.

**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 the FIPS 199 “moderate” system classification. The security controls and implementations are described in an up-to-date system security plan (SSP). This SSP describes the restrictions for access and disclosure to persons as authorized in the statute, provides administrative and management, physical, operational, and technical system control implementations.

Technical controls include access controls with strong passwords, tokens, PIV cards, encryption of data in transmission and at rest, RBAC, separation of duties, auditing tools and logs, monitoring and scanning for vulnerabilities. Intrusion detection systems, firewalls, Virtual Private Networks, and demilitarized zones (DMZs) are implemented and are provided by the Cloud Service Provider, AWS.

Physical controls include restricted access to facilities, secured system locations, and continued risk

assessments to ensure robust security posture. 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.

The system requires monitored access and OCSS promotes security training. All personnel with access to the system are required to sign the HHS Rules of Behavior, the OCSS Supplement to the HHS Rules of Behavior, and a non-disclosure oath upon completing security awareness training as a new hire and then annually.