US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/04/2016

OPDIV:

ACF

Name:

OCSE Data Reliability Audit (DRA) Electronic Information Collection

PIA Unique Identifier:

P-3450428-629898

The subject of this PIA is which of the following?

Electronic Information Collection

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

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?

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 Office of Child Support Enforcement (OCSE) Office of Audit is required by the Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA) and Section 452(a)(4)(C)(i) of the Social Security Act to complete Data Reliability Audits (DRA) and Data Reliability Review (DRRs) of states' performance indicator data. The purpose of these audits is to assess the completeness, reliability and security of states' systems that store and process the data reported on the Child Support Enforcement Annual Data Report Form (OCSE-157)) of the data in incentive payment systems. The data reliability audits and reviews are statutorily mandated for the purpose of allocating performance incentive funding to states. This requires receipt of electronic files from each state that contain the complete, unduplicated child support case universe, including all open IV-D cases, closed cases and non-IV-D cases, and the audit trails for each line on the Child Support Enforcement Annual Data Report Form (OCSE-157) used in the computation of performance indicators.

Every year, the OCSE Audit Team requires states to provide data covering a period of one year and to submit the data via encrypted files on Compact Diskette (CD) or Digital Versatile Diskette (DVD). The OCSE DRA Electronic Information Collection uploads this data via CD/DVD for the purpose of conducting these DRAs and data is collected, reviewed and temporarily maintained on full disk encrypted (FDE) government-owned computers.

Data testing is required to complete the annual DRA. A statistically valid, random sample of child support cases is selected from the information provided by each state. These cases are reviewed by inspecting hard copy documentation, logging into the state child support system at a state office or by using a state provided terminal in an OCSE office, via VPN or web-based access to the state system from our audit offices or a combination of these three options. State system access from our audit offices is accomplished on a FDE government-owned computer. Auditors typically view data elements Personally Identifiable Information (PII) identical to those initially provided by the state on the encrypted CD/DVD. Infrequently, an auditor may acquire additional, case-related PII in order to corroborate audit findings (consisting of potential source documents such a birth certificates, divorce decrees, or court orders). If this step is necessary, that additional information is converted to portable document format (PDF) and incorporated into the other audit files developed during the course of the audit. The initial state-level files, and subsequently developed audit files and final audit reports are zipped, encrypted and stored on an external hard drive. This data and information is maintained in the OCSE DRA Electronic Information Collection for approximately 10 years.

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

The OCSE DRA Electronic Information Collection collects, maintains and only shares internally with the OCSE Audit Team for state audit purposes only the following information derived from state-level child support case files: Case Identification (ID); case status; case status date; Custodial Parent Name; Non-Custodial Parent Name; paternity establishment date; amount due; amount distributed; child's name; child's birth date; complete parent's social security number (SSN) collected during the period of 2003 through 2005; and partial or redacted parent's SSN last four digits of the SSN for each parent and child collected during the period of 2008 through 2010. The OCSE Audit Team no longer collected SSN beginning in 2011. The system has no established interface and is not integrated with any external systems for the purpose of data and information exchange, upload, download or integration. The system is used solely to audit state data completeness and reliability only and to archive audit trails and working files. Data is received via encrypted CD/DVD that is loaded into the CD/DVD-drive of the Information Technology Infrastructure Operations (ITIO), HHS issued FDE computers and copied to the computer hard drive and copied to an external hard drive and encrypted via Federal Information Processing Standard (FIPS) 140-2 compliant whole-disk encryption software for long term storage and archive. In conducting the data testing portion of the audit, audit team members may acquire additional, case-related PII in order to corroborate audit findings (consisting of potential source documents such a birth certificates, divorce decrees, or court orders). If this step is necessary, that additional information is converted to .PDF and incorporated into the other audit files developed during the course of the audit. The initial state-level files, and subsequently developed audit files and final audit reports are zipped, encrypted and stored on an external hard drive. This data and information is maintained in the OCSE DRA Electronic Information Collection for approximately 10 years.

Audit Team members use ITIO, HHS issued computers that require end users to authenticate and logon via username and password (from four Non-Regional Offices) and Personal Identity Verification (PIV) Card (for Regional Offices). Information includes HHS official user credentials (HHS user name and password; and PIV credentials) for audit team leaders and audit team members on the ITIO issued computer. The HHS credentials are used to authenticate end users with the HHS network and are cached locally on the computer for logon to the computer during the auditing process. If the HHS user credentials have been deleted or locked by HHS network servers, users will not be authenticated.

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

The OCSE DRA Electronic Information Collection collects, maintains and only shares internally with the OCSE Audit Team for state audit purposes only the following information derived from state-level child support case files: Case Identification (ID); case status; case status date; Custodial Parent Name; Non-Custodial Parent Name; paternity establishment date; amount due; amount distributed; child's name; child's birth date; complete parent's social security number (SSN) collected during the period of 2003 through 2005; and partial or redacted parent's SSN last four digits of the SSN for each parent and child collected during the period of 2008 through 2010. The OCSE Audit Team no longer collected SSN beginning in 2011. The system has no established interface and is not integrated with any external systems for the purpose of data and information exchange, upload, download or integration. The system is used solely to audit state data completeness and reliability only and to archive audit trails and working files. Data is received via encrypted CD/DVD that is loaded into the CD/DVD-drive of the ITIO, HHS issued FDE computers and copied to the computer hard drive and copied to an external hard drive and encrypted via FIPS 140-2 compliant whole-disk encryption software for long term storage and archive. In conducting the data testing portion of the audit, audit team members may acquire additional, case-related PII in order to corroborate audit findings (consisting of potential source documents such a birth certificates, divorce decrees, or court orders). If this step is necessary, that additional information is converted to .PDF and incorporated into the other audit files developed during the course of the audit. The initial state-level files, and subsequently developed audit files and final audit reports are zipped, encrypted and stored on an external hard drive. This data and information is maintained in the OCSE DRA Electronic Information Collection for approximately 10 years.

The system collects information (both PII and non-PII) for DRAs and DRRs to determine whether State-reported data used to compute performance levels are complete and reliable. This audit determination can result in an incentive award or a financial penalty.

Audit Team members use ITIO, HHS issued computers that require end users to authenticate and logon via username and password (from four Non-Regional Offices) and Personal Identity Verification (PIV) Card (for Regional Offices). Information includes HHS official user credentials (HHS user name and password; and PIV credentials) for audit team leaders and audit team members on the ITIO issued computers. The HHS credentials are used to authenticate end users with the HHS network and are cached locally on the computer for logon to the computer during the auditing process. If the HHS user credentials have been deleted or locked by HHS network servers, users will not be authenticated.

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

Certificates

Legal Documents

The PII includes the following: case identification number, user credentials (username, password, and PIV credentials), birth certificates, divorce decrees, and court orders.

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

Employees

Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The PII is essential for establishing association between and among various data sets, documents, and records and elements (provided by the states to HHS) used for completing the audits.

User credentials (username and password, and PIV credential) are only used for end user authentication.

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

Not Applicable (N/A)

Describe the function of the SSN.

Full or partial SSNs are no longer collected, but are maintained to document audit trails during the 10 year data retention period.

Cite the legal authority to use the SSN.

The legal authority for using the SSN are contained in sections 453(a)(2)(A) and 453A(e) of the Social Security Act. Section 453(a)(2)(A) requires collection of SSN by HHS for child support enforcement purposes. Section 453A(e), State Case Registry, requiring states to collect standardized data elements such as the SSN to identify parties involved in a case for child support enforcement purposes. 45 Code of Federal Regulation (CFR) § 305.65(a) State cooperation in audit: requires states to make available to the Federal auditors such records or other supporting documentation (electronic and manual) as the audit staff may request, including records to support the data as submitted on the Federal statistical and financial reports that will be used to calculate the State's performance.

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

The Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA) and Section 452 (a)(4)(C)(i) of the Social Security Act require completion of the Data Reliability Audits (DRA) and Data Reliability Review (DRRs) and collection of states’ performance indicator data.

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

OMB Control Number: 0970-0177
EXPIRATION DATE: 09/30/2017

Is the PII shared with other organizations?

No

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

OCSE provides no initial notification to individuals that their personal information will be collected, because the original information for creating and establishing the case file is initiated and gathered at the state level.

Information is collected by the states. Any initial notification for the collection of the information is provided by the state.

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.

Case file information is collected at the State-level. At the time of collection, individuals are provided with the options of opting-out of creating a case file and collection of their PII. Any notification and determination not to participate in the child support enforcement process is handled at the state level.

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

Case file information is collected at the State-level. Any notification for the purpose of obtaining consent from the individuals whose PII is contained in the originating system when major changes occur to the system would be provided at the state level. There are no documented processes for states to notify HHS in the event of any PII concerns. HHS does not receive notification of PII data that have changed through periodic reconciliation conducted by the state.

At the Federal-level (HHS) no unauthorized disclosures are made outside of the OCSE DRA Electronic Information Collection.

End user account PII is collected by ITIO, HHS for the purpose of creating a credential for network and computer logon. Any notification for the purpose of obtaining consent from the individuals whose PII is contained in the originating system when major changes occur to the system would be provided by ITIO, HHS.

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.

Case file information is collected at the State-level and it is the responsibility of the States to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. There are no documented processes for states to notify HHS in the event of any PII concerns. HHS does not receive notification of PII data that have changed through periodic reconciliation conducted by the state. Individuals concerned with the accuracy of their PII would need to contact the state to address the issues of inappropriate use or disclosure.

At the Federal-level (HHS) no unauthorized disclosures are made outside of the OCSE DRA Electronic Information Collection.

End user account PII is collected by ITIO, HHS for the purpose of creating a credential for network and computer logon the computer issued by ITIO, HHS. It is the responsibility of ITIO, HHS to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

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 primary function and objective for establishing and using the annual OCSE DRA Electronic Information Collection is for review, evaluation and determination of data completeness, reliability and accuracy. A critical component of the audit process is use of the PII (specifically the SSN during the years it was collected) for establishing association between and among various data sets, documents, and records and elements (provided by the states to HHS) used for completing the audits. Any errors found during the audit process are reported to the state with recommendations for correction. States are encouraged to review their performance indicator data regularly to ensure the continued submission of data free of omissions, deficiencies, or other known errors, that may affect the accuracy and reliability of the performance indicators.

At the Federal-level (HHS) no unauthorized disclosures are made outside of the OCSE DRA Electronic Information Collection.

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

Users:

The PII is essential for establishing association between and among various data sets, documents, and records and elements (provided by the states to HHS) used for completing the DRAs/DRRs. The purpose of these audits is to assess the completeness, reliability and security of states' systems that store and process the data reported on the Child Support Enforcement Annual Data Report Form (OCSE-157)). Users include the Audit Team Leaders and Audit Team members who have equal access to the data at various stages of the audit process.

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

The OCSE Office of Audit and Audit Team leads determine audit team member roles and responsibilities, and authorizes and approve Audit Team member access to the OCSE DRA Electronic Information Collection. Access to the OCSE DRA Electronic Information Collection is further controlled by physical controls and the fact that the data is contained on CDs/DVDs and can only be accessed by uploading the information to an ITIO issued full disk encrypted computer. Unless physically granted access to the CD/DVD and with an authorized end user account on the ITIO computer used to conduct the DRAs/DRRs, access is controlled to the information and 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.

The electronic files from each state that contain the complete, unduplicated child support case universe, including all open IV-D cases, closed cases and non-IV-D cases, and the audit trails for each line on the Child Support Enforcement Annual Data Report Form (OCSE-157) used in the computation of performance indicators are the minimum and necessary information for OCSE Audit Team members to perform their jobs functions. Through the progressive process of conducting the DRAs, the OCSE has been able to identify only the essential information necessary for completing the audits, and has been able to effectively eliminate the use of SSN. Only the minimum required information is available to Audit Team members.

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, contractors, and other system users must review and sign an acknowledge statement of the HHS Rule of Behavior (Rob). This acknowledgment must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. All users of Privileged User accounts for Department information technology resources must read these standards and sign the accompanying acknowledgment form in addition to the HHS RoB before accessing Department data/information, systems, and/or networks in a privileged role. OCSE DRA Electronic Information Collection system 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.

Auditors also are required to comply with audit specific data retention and encryption policies

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

Audit Team Members provide direct hands-on training to new Audit Team members and they are provided with the Audit Team, OCSE SOP that informs them on proper handling, safeguarding and securing of sensitive data and information (specifically PII). Government Accountability Office Audit Standard 6.45 state that only auditors with the appropriate knowledge, skill and expertise be assigned to audits. Auditors are also required to receive 80 hours of training every two years. 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?

No

Describe the process and guidelines in place with regard to the retention and destruction of PII.

The program office is in communications with the ACF Records Manager to determine the specific 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 disposition 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.

Administrative Procedures:

Data collection involves use of a data de-identification process: originally SSN were redacted/masked to include only the last four digits of the SSN; subsequent procedures completely eliminated the use of the SSN

OCSE has established organizational wide policies, processes and procedures for whole-disk encryption to ensure oversight, management, and adherence to the established policies by field operations with specific focus on effective training and use of encryption technologies for safeguarding and securing sensitive HHS data and information on mobile media and devices. This policy ensures the use of external media, where files containing sensitive HHS data and information will only be accessed, opened, and used using devices/computers (desktop/laptop) with FDE technology employed on internal hard drives (completely eliminating the use of external media). OCSE policy requires that individual laptops will be locked in hardened safes/cabinets when not under direct physical control or use of OCSE staff.

Technical Controls:
ACF and the OCSE Program acquire information technology resources through the ITIO, HHS for computers. The computers are issued with FDE technology. OCSE uses the following software/encryption technologies to ensure encryption of external devices: CheckPoint Endpoint Security (CPES) or SecureZip for encrypting external media such as USB drives and portable computing devices compliant with FIPS 140-2 standards. OCSE auditors use ITIO-approved full-encrypting computers that incorporate ITIO-provided CheckPoint Endpoint encryption software that allows employees to cancel encryption when transferring files to external media. OCSE also acquires and uses USB media with built-in native encryption compliant with FIPS 140-2 standards (e.g. IMC KanguruDrive, Ironkey USB, or SanDisk Enterprise, etc.).
System computer access control and identity management via username and password (from four Non-Regional Offices) and Personal Identity Verification (PIV) Card (for Regional Offices). Information includes HHS official user credentials (HHS user name and password; and PIV credentials) for audit team leaders and audit team members on the ITIO issued computers.

Physical Controls:
OCSE acquired capabilities for physically safeguarding and securing the office (PIV card reader on entry door) and portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers) and implemented procedures for removing them and locking them in secure containers when not in use or direct physical control by OCSE staff (desk, hardened file cabinets, safes, etc.).