COMPUTER MATCHING AGREEMENT

BETWEEN

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES
OFFICE OF CHILD SUPPORT SERVICES

AND

STATE AGENCY ADMINISTERING
THE TEMPORARY ASSISTANCE FOR NEEDY FAMILIES PROGRAM

Verification of State TANF Eligibility

U.S Department of Health and Human Services Data Integrity Board #2503

On June 5, 2023, the Administration for Children and Families published a notice in the Federal Register at Volume 88, Number 107, Page 36587 to announce that the Office of Child Support Enforcement is now the Office of Child Support Services (OCSS). Any reference to OCSE has now been changed to OCSS and they are one and the same.

I. PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

This computer matching agreement ("agreement") governs a matching program between the U.S Department of Health and Human Services, Administration for Children and Families, Office of Child Support Services (OCSS), and the state agency administering the Temporary Assistance to Needy Families (TANF) program, hereinafter "state agency." This is a standard agreement between OCSS and all state agencies participating in the matching program. The state agency is the "non-federal agency" and OCSS is the "source agency" as defined by the Privacy Act. 5 U.S.C. § 552a(a)(10) and (11). OCSS and participating state agencies have entered into matching agreements and renewals for this matching program since 2005, the latest of which expires July 17, 2025 (*see* Appendix A). This agreement includes a security addendum and a cost-benefit analysis (*see* Appendix B).

A. Purpose of the Matching Program

The Privacy Act of 1974 ('Privacy Act") requires that each matching agreement specify the purpose and legal authority for conducting the matching program. 5 U.S.C. § 552a (o)(1)(A).

The purpose of the matching program is to help the state agency establish or verify individuals' eligibility for benefits under the TANF program. OCSS will provide the state agency with new hire, quarterly wage, and unemployment insurance information from the

National Directory of New Hires (NDNH) pertaining to individuals identified by the state agency who are adult applicants for, or recipients of, help under the TANF program.

The state agency may also use the NDNH information for updating applicants' and recipients' reported participation in work activities and updating contact information maintained by the state agency about applicants and recipients and their employers.

The definition of a "matching program" in the Privacy Act at 5 U.S.C. § 552a(a)(8)(A)(i)(I) and (II) includes a computerized comparison of two or more automated systems of records with non-federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of service with respect to, cash or in-kind assistance or payments under a federal benefit program, or to recoup payments or delinquent debts under those programs. Records may not be disclosed from a system of records to a recipient agency or non-federal agency for use in a matching program except pursuant to a written agreement containing the provisions specified in the Privacy Act at 5 U.S.C. § 552a(o).

B. Legal Authority

Subsection 453(j)(3) of the Social Security Act provides the legal authority for conducting the matching program.

In pertinent part, subsections 453(j)(3)(A) and (B) state:

> To the extent and with the frequency that the Secretary determines to be effective in assisting States to carry out their responsibilities under programs operated under this part, part B, or part E and programs funded under part A, the Secretary shall:
>
> > (A) compare the information in each component of the Federal Parent Locator Service maintained under this section against the information in each other such component (other than the comparison required by paragraph (2)), and report instances in which such a comparison reveals a match with respect to an individual to State agencies operating such programs; and
> >
> > (B) disclose information in such components to such State agencies.
>
> 42 U.S.C. § 653(j)(3).

C. Definitions

The following terms contained in this agreement will have the meaning given such terms in subsection (a) of the Privacy Act, 5 U.S.C. § 552a(a):

(1) "Federal benefit program" means any program administered or funded by the federal government, or by any agent or state on behalf of the federal government,

providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

(2) "Individual" means a citizen of the United States or an alien lawfully admitted for permanent residence.
(3) "Maintain" means to maintain, collect, use or disseminate.
(4) "Matching program" means any computerized comparison of two or more automated systems of records or a system of records with non-federal records. The comparison outcomes are used to help establish or verify benefit eligibility for services, such as cash or in-kind assistance, under federal benefit programs and to recover delinquent debts or payments made in error under federal benefit programs, or both.
(5) "Non-federal agency" means any state or local government, or agency of it, which receives records contained in a system of records from a source agency for use in a matching program.
(6) "Recipient agency" means any agency, or contractor of it, receiving records contained in a system of records from a source agency for use in a matching program.
(7) "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including the individual's education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
(8) "Routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.
(9) "Source agency" means any agency which discloses records contained in a system of records to be used in a matching program, or any state or local government, or agency thereof, which discloses records to be used in a matching program.
(10) "System of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Additional terms used in this agreement are defined as follows:

(11) "Federal Parent Locator Service" (FPLS) means a service, which includes the NDNH, conducted under the direction of OCSS pursuant to section 453 of the Social Security Act for purposes specified in sections 453 and 463.
(12) "National Directory of New Hires" (NDNH) means an automated directory maintained in the FPLS, established by subsection 453(i)(1) of the Social Security Act, containing new hire, unemployment compensation, and quarterly wage information supplied by state and federal agencies pursuant to subsections 453A(b)(1)(C) and (g)(2) of the Social Security Act.
(13) "New hire information" means employer information pertaining to newly hired employees reported to the NDNH by state and federal agencies pursuant to subsections 453A(b)(1)(C) and (g)(2)(A), and 453(i)(1) of the Social Security Act.

(14) "Quarterly wage information" means wage information reported to the NDNH by state and federal agencies pursuant to subsections 453A(g)(2)(B) and 453(i)(1) and (n) of the Social Security Act.
(15) "Unemployment compensation information" means information pertaining to benefits paid under state unemployment compensation programs and reported to the NDNH pursuant to subsections 453A(g)(2)(B)and 453(e)(3) and (i)(1) of the Social Security Act.
(16) "Secretary" means the Secretary of the U.S. Department of Health and Human Services, unless otherwise provided specifically in the agreement. For the purposes of the Federal Parent Locator Service established under 42 U.S.C § 653, the Secretary has delegated operational responsibilities to OCSS.
(17) "Adult" means an individual who is not a minor child.

Any additional term definitions found in the TANF regulations at 45 CFR § 260.30 are incorporated by reference.

II. JUSTIFICATION AND ANTICIPATED RESULTS

The Privacy Act requires that each matching agreement specify the justification for the program and the anticipated results, including a specific estimate of any savings. 5 U.S.C. § 552a(o)(1)(B).

A. Cost-Benefit Analysis

Unless statutorily excepted or waived by the HHS Data Integrity Board (DIB), a cost-benefit analysis must be completed and submitted to the DIB to consider in determining whether to approve the matching program. If the analysis does not demonstrate that the matching program is likely to be cost effective, the DIB may approve the matching agreement based on other supporting justifications. *See* 5 U.S.C. § 552a(u)(4)(A) through (C) and Office of Management and Budget (OMB) guidance in *Privacy Act of 1974: Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1998,* 54 FR 25818 (June 19, 1989), at pages 25821 and 25828-25829.

Eight states participated in the 2023 matching program, and five states provided performance outcome reports to OCSS. The current cost-benefit analysis (Appendix B) is derived from the fees the five states paid and cost savings calculations from the five states' performance outcomes reports. The combined cost for the five state agencies is less than the combined savings they identified from the first month in which applicants' and recipients' information was compared to information in the NDNH.

B. Other Supporting Justifications

OMB has identified the TANF program as susceptible to significant improper payments. This matching program supports compliance with the requirements set forth in E.O. 13520, *Reducing Improper Payments and Eliminating Waste in Federal Programs*, 74 FR 62201 (Nov. 25, 2009) and enacted into law through the Payment Integrity Information Act of

2019. The guidance and law requires federal programs that determine eligibility and provide benefits to their applicants and recipients to have policies in place that provide transparency and public scrutiny of significant payment errors; focus on eliminating the highest improper payments; establish accountability for reducing improper payments; coordinate federal, state, and local government action in identifying and eliminating improper payments; and implement guidelines in Appendix C to Circular A-123, as amended .(OMB Memorandum M-21-19, *Transmittal of Appendix C to Circular A-123, Requirements for Payment Integrity Improvement* (March 5, 2021)). Payment integrity is a top priority and OMB guidance provides the framework to reduce the administrative burden, allowing agencies to focus on identifying, assessing, prioritizing, and responding to payment integrity risks and the underlying causes of improper payments. The matching program also facilitates compliance with the applicable requirements of 31 U.S.C. §§ 3351-3358.

Because the NDNH is a centralized database of wage and employment information and provides an effective and efficient means to obtain income information, it is preferable to other means of obtaining the same information. Identifying employment status and wages of adult TANF applicants and recipients helps the state agency to provide proper case management and work supports to stabilize employment, increase earnings, reduce dependency on public assistance, and lead to self-sufficiency. The program also improves the state agency's ability to report adult TANF applicants' and recipients' employment status and earnings and work participation to the Office of Family Assistance, in accordance with subsection 411(a)(1)(A)(iv) and (xi) of the Social Security Act. 42 U.S.C. § 611(a)(1)(A)(iv) and (xi).

The matching program assists the participating state agency in detecting fraud, waste, and abuse and enhances program integrity by strengthening the state agency's oversight and management of the TANF program. It serves as a deterrent to some individuals who otherwise may fraudulently apply for and receive TANF benefits and provides information to reduce erroneous payments. The program also provides useful information on the employment and earnings of TANF applicants and recipients, specifically: 1) those who are employed with the federal government; 2) those who are employed in another state, including those who have been rehired by a previous employer after having been separated from such prior employment for at least 60 consecutive days (Pub. L. 112-40, effective April 21, 2012, amending subsection 453A(a)(2) of the Social Security Act, 42 U.S.C. § 653a(a)(2)); and 3) those whose information is not readily available through the State Directory of New Hires, state workforce agencies, or other data reporting systems or sources.

The positive results of the previous matching programs conducted between the state agency and OCSS under previous matching agreements further justify re-establishing the matching program under this agreement. *See* section II.A and the cost-benefit analysis at Appendix B to this agreement.

C. Specific Estimate of Any Savings

The cost-benefit analysis (*See* Appendix B), derived from the performance outcomes reports submitted by five of the eight participating state agencies, demonstrates that the matching

program helped states to determine eligibility and avoid improper payments. After verification of previously unkown earnings, state agencies collectively reported 1,621 cases that were either closed or had benefits reduced, which collectively avoided approximately $358,119 in improper payments. The parties to this agreement anticipate that savings and operational benefits derived from the NDNH matching program will continue.

III. RECORDS DESCRIPTION

The Privacy Act requires that each matching agreement specify a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program. 5 U.S.C. § 552a(o)(1)(C).

A. Sources of the Records Used in This Matching Program

1. OCSS System of Records

OCSS will disclose match results to the state agency from the following system of records: *OCSS National Directory of New Hires,* System No. 09-80-0381; *see* System of Records Notice (SORN) published in full at 89 FR 25625 (April 11, 2024). The disclosure of NDNH records by OCSS to the state agency is authorized by routine use (8) published in the NDNH SORN. 89 FR 25625, 25629 (April 11, 2024).

2. State Agency Records

The state agency records used in the information comparison contain information collected by the state agency in its administration of its TANF program, according to federal law. Subsections 1137(a) and (b)(1) of the Social Security Act require an applicant for, or recipient of, federal benefits, including TANF benefits, to furnish an identifying number, such as a tax identifier or Social Security number as a condition of eligibility.

42 U.S.C. § 1320b-7(a)(2) and (b)(1), 31 U.S.C. § 7701(c)

B. Number of Records Involved

The combined monthly caseload of all state TANF programs is approximately 1.1 million TANF applicants and recipients. The input file provided to OCSS by the state agency will contain records representing a portion of that state's caseload. Each state agency's agreement signature page provides the estimated number of records to be submitted to OCSS by the state agency.

The approximate number of records in the output file provided to the state agency by OCSS will depend upon the number of individuals whose information is maintained in the NDNH and the amount of NDNH information, if any, associated with those individuals.

C. Specified Data Elements Used in the Match

1. Data Elements in the State Agency Input File

The state agency input file provided to OCSS must be programmed according to the TANF-NDNH matching program record specifications for successful transmission and comparison. The file will contain records pertaining to individuals who are adult TANF applicants for or recipients of TANF benefits and will contain each individual's name and Social Security number.

Additionally, the state agency may include alpha-numeric characters in the Passback Data field of the Input Detail Records to identify the purpose for which the record is being submitted for NDNH matching. The state agency may also indicate whether the state agency requests NDNH new hire, quarterly wage, or unemployment insurance even if the information was provided by that same state.

As provided in the TANF-NDNH Record Specifications, OCSS will verify the name and SSN combinations in the state agency's input file using Social Security Administration processes. Any records that do not pass the verification process will be rejected and the output file will include notification with an explanation for the failure.

2. NDNH Data Elements

To accomplish the purpose of this matching program, the state agency will request the following data elements from the NDNH new hire, quarterly wage, and unemployment insurance files. The file provided to the state agency by OCSS will contain the requested new hire, quarterly wage, and unemployment insurance information, if any, pertaining to the individuals whose SSNs are contained in the state agency input file. The file will also contain a code indicating why a record was rejected, if applicable.

a. New Hire File

- New hire processed date
- Employee name
- Employee address
- Employee date of hire
- Employee state of hire
- Federal Employer Identification Number
- State Employer Identification Number
- Department of Defense code
- Employer name
- Employer address
- Transmitter agency code
- Transmitter state code
- Transmitter state or agency name

b. Quarterly Wage File

- Quarterly wage processed date
- Employee name
- Federal Employer Identification Number
- State Employer Identification Number
- Department of Defense code
- Employer name
- Employer address
- Employee wage amount
- Quarterly wage reporting period
- Transmitter agency code
- Transmitter state code
- Transmitter state or agency name

c. Unemployment Insurance File

- Unemployment insurance processed date
- Claimant name
- Claimant address
- Claimant benefit amount
- Unemployment insurance reporting period
- Transmitter state code
- Transmitter state or agency name

D. Frequency of Data Exchanges

Subsection 453(j)(3) of the Social Security Act requires comparison and disclosure to assist states to carry out their responsibilities under TANF to the extent and with the frequency that the Secretary determines to be effective. 42 U.S.C. § 653(j)(3).

The Secretary has determined that comparisons and disclosures at a frequency established by the state agency are effective in assisting states to carry out responsibilities under TANF. The state agency requests monthly comparisons and disclosures of new hire, quarterly wage, and unemployment insurance information.

E. Projected Start and Completion Dates

The projected start date of this agreement is July 19, 2025, and the projected expiration date is January 18, 2027 (18 months from the start date). The parties may, within three months prior to the expiration date of this agreement, renew the agreement for a period of up to one year, if the requirements stated in section XII.A are met, which would make the expiration date of this agreement January 18, 2028.

IV. NOTICE PROCEDURES

A. Individualized Notice that Information May Be Subject to Verification through Matching Programs

The Privacy Act requires that the matching agreement specify procedures for providing individualized notice at the time of application, and periodically thereafter, subject to guidance provided by the Director of the Office of Management and Budget, to applicants for and recipients of financial assistance or payments under federal benefit programs, that any information provided by such applicants and recipients may be subject to verification through matching programs. 5 U.S.C. § 552a(o)(1)(D)(i).

Pursuant to this requirement, the state agency has implemented procedures and developed forms for providing individualized notice at the time of application and periodically thereafter. The notice informs applicants or recipients that the information they provide may be verified through matching programs. The notification methods include, but are not limited to, a statement on the initial application for TANF assistance (hard copy and electronic); an explanation in the benefit program handbook provided at the time of application; a banner on the state agency website for TANF applicants and TANF recipients; and a statement in letters to applicants and recipients of TANF assistance.

B. Constructive Notice of Matching Program

The Privacy Act requires federal agencies to publish notice of the establishment or revision of a matching program with a non-federal agency in the *Federal Register* for public notice and comment, at least 30 days prior to conducting such program. 5 U.S.C. § 552a(e)(12).

OCSS will publish the required public notice of the matching program in the *Federal Register* at least 30 days before conducting the program under this agreement and will make the notice and this agreement available on the HHS computer matching agreement (CMA) internet site as required by OMB Memorandum M-17-06 *Policies for Federal Agency Public Websites and Digital Services* (November 8, 2016). The *Federal Register* notice will provide constructive notice of the matching program to affected individuals. OCSS will not publish the *Federal Register* notice until OCSS has reported the matching program to the Office of Management and Budget (OMB) and Congress for advance review and OMB has completed its review as required by 5 U.S.C. § 552a(o)(2)(A) and (r) and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, 81 FR 94424 (Dec. 23, 2016), at pages 17-23.

V. VERIFICATION PROCEDURES AND OPPORTUNITY TO CONTEST FINDINGS

The Privacy Act at 5 U.S.C. § 552a(o)(1)(E) requires that each matching agreement specify procedures for verifying information produced in the matching program and for providing affected individuals an opportunity to contest findings before an adverse action is taken against them. State agencies must comply with the following requirements:

A. Verification Procedures

Subsection (p) of the Privacy Act provides as follows:

(1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until

(A)(i) the agency has independently verified the information; or . . .

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C)(i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or
(ii) in the case of a program for which no such period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of –

(A) the amount of any asset or income involved;
(B) whether such individual actually has or had access to such asset or income for such individual's own use; and
(C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

5 U.S.C. § 552a(p).

Thus, to comply with the Privacy Act, the state agency understands that information obtained from the NDNH is not conclusive evidence of the address, employment, and financial information of an identified individual and that it must, in accordance with 5 U.S.C. § 552a(p)(2), independently verify the NDNH information before taking adverse action to deny, reduce, or terminate benefits. State agencies have procedures to verify the current employment and income status of the applicant or recipient before taking action, which include, but are not limited to, notification of third parties, such as named employers or other state agencies, and calls to the applicant or recipient. These verification procedures and methods vary from state to state, as do the methods for notification of such findings, which include letters to applicants and recipients of TANF assistance advising them of possible pending action.

Further, subsection (q)(1) of the Privacy Act provides that, notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency or non-federal agency for a matching program if such source agency has reason to believe that the verification and opportunity to contest requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency. 5 U.S.C. § 552a(q)(1). *See also* the Office of Management and Budget guidelines *Privacy Act of 1974: Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1998*, 54 FR 25818 (June 19, 1989), at pages 25827, 25829.

OCSS verifies information in the NDNH to ensure accuracy of records (*see* section IX). Records in an NDNH output file disclosed by OCSS to a state agency will indicate whether each name and SSN combination in the match results obtained from the NDNH has been verified for accuracy. OCSS verification procedures and output file indicators increase the likelihood that the NDNH information OCSS provides to the state agency will pertain to the appropriate individuals.

B. Opportunity to Contest Findings

The state agency must have established and implemented procedures to notify the individual of the findings resulting from NDNH information and provide an opportunity to contest the findings by a specified date before the state agency may take adverse action.
5 U.S.C. § 552a(p)(1)(B) and (C).

VI. DISPOSITION OF MATCHED ITEMS

The Privacy Act requires that each matching agreement specify procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-federal agency in such matching program. 5 U.S.C. § 552a(o)(1)(F). The Privacy Act also requires that each matching agreement specify procedures governing the use by the recipient agency or non-federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program. 5 U.S.C. § 552a(o)(1)(I).

The following provisions specify the retention periods for the records contained in the input file provided by the state agency and for the NDNH records in the output file provided by OCSS, including any electronic copies or paper printouts of the records in those files, even copies or printouts of NDNH records that are not labeled as NDNH records. Electronic files and information and any paper printouts must be disposed of as provided in the Security Addendum at III. 23. and 28.

A. State Agency Records in the Input File

OCSS may retain the records contained in the input file provided to OCSS by the state agency only for the period of time required for any processing related to the matching program, but no longer than 60 days after the transmission of the file to OCSS.

B. NDNH Records in the Output File

1. Copy of NDNH Records in the Output File

OCSS may retain copies of the records contained in the NDNH output file that OCSS provides to the state agency only for the period of time required to ensure the successful transmission of the output file to the state agency, but no longer than 60 days after the transmission of the output file to the state agency.

2. NDNH Records in Output File Provided to State Agency

The state agency may retain NDNH records contained in the output file OCSS provided to the state agency only for the period of time required to achieve the authorized purpose of the matching program, but no longer than two years from the date of the OCSS disclosure of the files to the state agency.

VII. SECURITY PROCEDURES

The Privacy Act requires that each matching agreement specify procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs. 5 U.S.C. § 552a(o)(1)(G). Federal agencies must ensure that state agencies afford the appropriate equivalent level of security controls as maintained by the federal agency. *See* OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy* (December 20, 2000).

The procedures and controls to ensure the appropriate equivalent level of security for records matched and the results of such programs are specified in the security addendum to this agreement.

VIII. RECORDS USAGE, DUPLICATION, AND REDISCLOSURE RESTRICTIONS

The Privacy Act requires that each matching agreement specify prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or non-federal agency, except where provided by law or essential to the conduct of the matching program. 5 U.S.C. § 552a(o)(1)(H). The Privacy Act also requires that each matching agreement specify procedures governing the use by a recipient agency or non-federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program. 5 U.S.C. § 552a(o)(1)(I).

Restrictions on duplication, redisclosure, and use of records are also found in the Social Security Act. Subsection 453(l)(1) requires that NDNH information and the results of comparisons using NDNH information shall not be used or disclosed except as expressly provided in section 453, subject to section 6103 of the Internal Revenue Code of 1986. 42 U.S.C. § 653(l)(1). Subsection 453(l)(2) provides that an administrative penalty (up to and including dismissal from employment) and a fine of $1,000 shall be imposed for each act of unauthorized access to, disclosure of, or use of, information in the NDNH by any officer or employee of the United States or any other person who knowingly and willfully violates the requirement. 42 U.S.C. § 653(l)(2). Subsection 453(m) requires the Secretary of the U.S. Department of Health and Human Services to establish and implement safeguards with respect to the entities established under this section designed to restrict access to confidential NDNH information to authorized persons and restrict use of such information to authorized purposes. 42 U.S.C. § 653(m)(2).

OCSS must use state agency records solely as provided in this agreement and must not duplicate or redisclose those records within or outside of OCSS. The state agency must use the results of the information comparison solely for the purposes authorized pursuant to this agreement and in accordance with the terms and conditions specified in this agreement, including the security addendum. The state agency may not redisclose or duplicate the results of the information comparison; however, if a state agency determines that redisclosure to a specified entity is essential to accomplishing the matching program's purposes (as specified in section I.), the state agency must obtain OCSS's written approval prior to any redisclosure. The state agency must submit a written request to OCSS describing the purpose, manner, and frequency of the proposed duplication or redisclosure and the entities to which such redisclosure is to be made. The state agency must certify that it will ensure that the proposed recipient has the appropriate equivalent level of security controls in place to safeguard the NDNH information. OCSS must review any such request and advise the state agency whether the request is approved or denied.

IX. RECORDS ACCURACY ASSESSMENTS

The Privacy Act requires that each matching agreement specify information on assessments that have been made on the accuracy of the records that will be used in the matching program. 5 U.S.C. § 552a(o)(1)(J).

A. NDNH Records

The information maintained within the NDNH is reported to OCSS by state and federal agencies. OCSS verifies the accuracy of name and SSN combinations maintained by OCSS against Social Security Administration databases in accordance with 42 U.S.C. § 653(j)(1). A record reported to the NDNH is considered "verified" if the name and SSN combination has a corresponding name and SSN combination within Social Security Administration databases.

One hundred percent of the employee name and SSN combinations contained in the new hire and the unemployment insurance files in the NDNH have been verified against Social Security Administration databases. For quarterly wage, 94 percent of name and SSN combinations have been verified because some states do not collect enough name data. However, information comparisons may be conducted and reliable results obtained.

B. State Agency Records

OCSS verifies state TANF agency records before conducting an information comparison with the NDNH (*see* section III.C.1), therefore name and SSN combinations within the state agency records have a high degree of accuracy.

X. COMPTROLLER GENERAL ACCESS

The Privacy Act requires that each matching agreement specify that the Comptroller General of the United States may have access to all records of a recipient agency or a non-federal agency that the Comptroller General deems necessary to monitor or verify compliance with this agreement. 5 U.S.C. § 552a(o)(1)(K). OCSS and the state agency agree that the Comptroller General may have access to such records for the authorized purpose of monitoring or verifying compliance with this agreement.

XI. REIMBURSEMENT/FUNDING

Subsection 453(k)(3) of the Social Security Act requires a state or federal agency that receives information from the Secretary to reimburse the Secretary for costs incurred by the Secretary in furnishing the information. The reimbursement shall be at rates which the Secretary determines to be reasonable and will include the costs of obtaining, verifying, maintaining, and comparing the information. 42 U.S.C. § 653(k)(3).

OCSS has established a full-cost reimbursement methodology for calculating user fees for each state or federal agency receiving information from the NDNH. A reimbursement agreement must be executed each federal fiscal year in which this computer matching agreement is in effect and if the state agency participates in the match. The state agency must reimburse OCSS in accordance with the terms of such reimbursement agreement.

XII. DURATION OF AGREEMENT

A. Effective Date of the Agreement

As stated in III.E., the State Agency and OCSS intend that the effective date of this agreement will be July 19, 2025, the day after the expiration date of the renewal of the prior matching agreement, No. 2206, and intend for this agreement to remain in effect for 18 months as permitted by 5 U.S.C. § 552a(o)(2)(C).

OCSS and the state agency may commence comparisons and disclosures under this agreement upon completion of all of the following requirements:

- OCSS and the authorized state agency officials sign the agreement.
- The HHS DIB approves this matching agreement and the HHS DIB Chairperson signs the agreement.
- The state agency submits the documentation required by OCSS to assess the security posture of the state agency.
- OCSS reports the matching program to OMB and Congress for their advance review and, upon completion of OMB's advance review, OCSS publishes the matching notice in the *Federal Register* for 30 calendar days, as required by 5 U.S.C. § 552a(e)(12), (o)(2)(A) and (r) and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, 81 FR 94424 (Dec. 23, 2016), at pages 17-23.

Within three months prior to the expiration date of this agreement the parties may renew the agreement for a period of up to one year if 1.) the program will be conducted without any change, 2.) each party to the agreement certifies to the DIB in writing that the program has been conducted in compliance with the agreement as permitted by 5 U.S.C. § 552a(O)(2)(D), and 3.) the agencies meet the requirement that no source agency may renew a matching agreement unless the recipient agency or non-federal agency has certified that it has complied with the provisions of that agreement and the source agency has no reason to believe that the certification is inaccurate. 5 U.S.C. § 552a(q)(2).

OCSS anticipates the matching program will meet renewal requirements and, upon HHS DIB Chairperson's signature, OCSS will distribute the approved CMA Renewal to the state agencies.

B. Modification of the Agreement

This agreement may be modified at any time by a written amendment which is approved by the state agency, OCSS, and the HHS DIB Chairperson. If any significant changes are needed, a new agreement will be required.

C. Termination of the Agreement

This agreement may be terminated at any time with the consent of OCSS and the state agency or unilaterally by either OCSS or the state agency upon written notice to the other. The termination date will be effective 90 days after the date of the notice or at a later date specified in the notice provided this date does not exceed the approved duration of the agreement.

If OCSS has reason to believe that any requirement of this agreement is not being met by the state agency, OCSS must terminate disclosures of records contained in the NDNH to the state agency, in accordance with subsection 552a(q)(1) of the Privacy Act. 5 U.S.C. § 552a(q)(1).

If OCSS determines that any authorized entity to which NDNH information is redisclosed by the state agency is not complying with any of the terms and provisions in this agreement, OCSS may terminate this agreement.

If OCSS determines that the privacy or security of NDNH information is put at risk by the state agency or any authorized entity, OCSS may terminate the agreement and any further disclosures to that state agency or authorized entity without prior notice.

XIV. PERIODIC REPORTING OF PERFORMANCE OUTCOMES

The Office of Management and Budget requires OCSS to periodically report measures of the performance of the FPLS, including the NDNH, through various federal management devices, such as the Office of Management and Budget Information Technology Dashboard, the Annual Report to Congress, and the Major IT Business Case. OCSS is required to provide performance measures demonstrating how the FPLS supports OCSS's strategic mission, goals and objectives, and cross-agency collaboration. OCSS also requests such performance reporting to ensure matching partners use NDNH information for the authorized purpose.

To assist OCSS in its compliance with federal reporting requirements and to provide assurance that the state agency uses NDNH information for the authorized purpose, the state agency must provide the OCSS with performance outcomes attributable to its use of NDNH information for the purposes set forth in this agreement.

OCSS will also use the performance reports to develop a cost-benefit analysis of the matching program, which is required for any subsequent matching agreements in accordance with 5 U.S.C. § 552a(o)(1)(B). *See* section II.B.

The state agency must provide such reports to OCSS annually, in a format determined by OCSS and approved by OMB as required by under the Paperwork Reduction Act, no later than three months after the end of each fiscal year of the matching program.

XV. PERSONS TO CONTACT

A. The U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Services contact for programs is:

Angela Kasey-Henry, Data Access Federal Oversight Manager
Division of Federal Systems
Office of Child Support Services
Administration for Children and Families
Mary E. Switzer Building
330 C Street, SW
Washington, DC 20201
Phone: 202-401-5568
Email: Angela.Kasey-Henry@acf.hhs.gov

B. The contacts on behalf of the state agency are:

[NAME]
[TITLE]
[AGENCY]
[MAILING ADDRESS]
[CITY, STATE, ZIP CODE]
Phone: [XXX-XXX-XXXX]
Email: [EMAIL ADDRESS]

[NAME]
[TITLE]
[AGENCY]
[MAILING ADDRESS]
[CITY, STATE, ZIP CODE]
Phone: [XXX-XXX-XXXX]
Email: [EMAIL ADDRESS]

XVI. APPROVALS

The authorized officials, whose signatures appear below, accept and expressly agree to the terms and conditions expressed herein, confirm that no verbal agreements of any kind will be binding or recognized, and hereby commit their respective organizations to the terms of this agreement.

A. U. S. Department of Health and Human Services Program Official

/s	
Linda Boyer Deputy Commissioner Office of Child Support Services	**Date**

B. U.S. Department of Health and Human Services Approving Official

/s	
Andrew Gradison Acting Assistant Secretary Administration of Children and Families	**Date**

C. U. S. Department of Health and Human Services Data Integrity Board

/s	
Scott W. Rowell Acting Chairperson	**Date**

D. State Agency Official

The state of _____ will submit approximately _____ records in each input file, which represent approximately _____individuals, at the frequency specified in section III.D. This number is an estimate of the number of records provided to OCSS by the state agency and may fluctuate within the effective period of the agreement.

[Name of State Agency Authorized Official] [Title of State Agency Authorized Official]	**Date**

SECURITY ADDENDUM

U.S. Department of Health and Human Services
Administration of Children and Families
Office of Child Support Services

and

State Agency Administering
the
Temporary Assistance for Needy Families Program

Verification of State TANF Eligibility

I. PURPOSE AND EFFECT OF THIS SECURITY ADDENDUM

The purpose of this security addendum is to specify the security controls that the Office of Child Support Services (OCSS) and the state agency administering Temporary Assistance for Needy Families Program (state agency) must have in place to ensure the security of the records compared against records in the National Directory of New Hires (NDNH), and the results of the information comparison.

By signing this security addendum, OCSS and the state agency agree to comply with the security requirements established by the U.S. Department of Health and Human Services and OCSS. OCSS and the state agency agree to use the information for authorized purposes in accordance with the terms of the computer matching agreement (agreement) between the state agency and OCSS.

OCSS may update this security addendum to address process or technology changes, as well as new or revised federal security requirements and guidelines. In such instances, OCSS must provide the state agency with written notification of such changes and require written assurance by the state agency that it must comply with new or revised security requirements.

II. APPLICABILITY OF THIS SECURITY ADDENDUM

This security addendum is applicable to the agency, personnel, facilities, documentation, information, electronic and physical records, other machine-readable information, and the information systems of OCSS and the state agency, and state agency authorized entities (such as contractors and entities specified in the agreement), which are hereinafter "OCSS" and "state agency."

III. SECURITY AND PRIVACY SAFEGUARDING REQUIREMENTS

The safeguarding requirements in this security addendum are drawn from the *Office of Child Support Services Division of Federal Systems Security Requirements for State Agencies Receiving National Directory of New Hires Data*. This document is available upon request from OCSSsecurity@acf.hhs.gov.

This section provides the safeguarding requirements with which OCSS and the state agency must comply and continuously monitor. The state agency must also comply with three additional requirements: Breach Reporting and Notification Responsibility; Security Certification; and Audit Requirements.

The safeguarding requirements for receiving NDNH information as well as the safeguards in place at OCSS for protecting the agency input files are as follows:

1. The state agency must restrict access to, and disclosure of, NDNH information to authorized personnel who need NDNH information to perform their official duties in connection with the authorized purposes specified in the agreement.

   OCSS restricts access to and disclosure of the agency input files to authorized personnel who need them to perform their official duties as authorized in this agreement.

   Policy/Requirements Traceability: 5 U.S.C. § 552a(b)(1), NIST SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations,* AC-3, AC-6

2. The state agency must establish and maintain an ongoing management oversight and quality assurance program to ensure that only authorized personnel have access to NDNH information.

   OCSS management oversees the use of the agency input files to ensure that only authorized personnel have access.

   Policy/Requirements Traceability: 5 U.S.C. § 552a; NIST SP 800-53 Rev 5, PL-4(1), PS-6, PS-8

3. The state agency must advise all authorized personnel who will access NDNH information of the confidentiality of NDNH information, the safeguards required to protect NDNH information, and the civil and criminal sanctions for non-compliance contained in the applicable state and federal laws, including section 453(l)(2) of the Social Security Act. 42 U.S.C. § 653(l)(2).

OCSS advises all personnel who will access the agency input files of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable federal laws.

Policy/Requirements Traceability: 5 U.S.C. § 552a; NIST SP 800-53 Rev 5, PL-4(1), PS-6, PS-8

4. The state agency must deliver security and privacy awareness training to personnel with authorized access to NDNH information and the system that houses, processes, or transmits NDNH information. The training must describe each user's responsibility for proper use and protection of NDNH information, how to recognize and report potential indicators of insider threat, and the possible sanctions for misuse. All personnel must receive security and privacy awareness training before accessing NDNH information and at least annually thereafter. The training must cover the matching provisions of the federal Privacy Act, the Computer Matching and Privacy Protection Act, and other state and federal laws governing use and misuse of NDNH information.

   OCSS delivers security and privacy awareness training to personnel. The training describes each user's responsibility for proper use and protection of other agencies' input files, how to recognize and report potential indicators of insider threat, and the possible sanctions for misuse. All personnel receive security and privacy awareness training before accessing agency input files and at least annually thereafter. The training covers the other federal laws governing use and misuse of protected information.

   Policy/Requirements Traceability: 5 U.S.C. § 552a; 44 U.S.C. § 3551 et seq; OMB Circular A-130, *Managing Information as a Strategic Resource*; OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information;* NIST SP 800-53 Rev 5, AT-2(2), AT-3

5. The state agency personnel with authorized access to NDNH information must sign non-disclosure agreements, rules of behavior, or equivalent documents before system access, annually, and if changes in assignment occur. The non-disclosure agreement, rules of behavior, or equivalent documents must outline the authorized purposes for which the state agency may use NDNH information, the privacy and security safeguards contained in this agreement and security addendum, and the civil and criminal penalties for unauthorized use. The state agency may use "wet" and/or electronic signatures to acknowledge non-disclosure agreements, rules of behavior, or equivalent documents.

   OCSS personnel with authorized access to the agency input files sign non-disclosure agreements and rules of behavior annually.

Policy/Requirements Traceability: OMB Circular A-130 – Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*; OMB M-17-12; NIST SP 800-53 Rev 5, PS-6

6. The state agency must maintain records of authorized personnel with access to NDNH information. The records must contain a copy of each individual's signed non-disclosure agreement, rules of behavior, or equivalent document and proof of the individual's participation in security and privacy awareness training. The state agency must make such records available to OCSS upon request.

   OCSS maintains a record of personnel with access to the agency input files. The records contain a copy of each individual's signed non-disclosure agreement, rules of behavior, or equivalent document and proof of the individual's participation in security and privacy awareness training.

   Policy/Requirements Traceability: NIST SP 800-53 Rev 5, AT-4

7. The state agency must have appropriate procedures in place to report confirmed and suspected security or privacy incidents (unauthorized use or disclosure involving personally identifiable information), involving NDNH information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state agency must report confirmed and suspected incidents, in either electronic or physical form, to OCSS, as designated in this security addendum. The requirement for the state agency to report confirmed or suspected incidents involving NDNH information to OCSS exists in addition to, not in lieu of, any state agency requirements to report to the United States Computer Emergency Readiness Team (US-CERT).

   OCSS has appropriate procedures in place to report security or privacy incidents, or suspected incidents involving the agency input files. Immediately upon discovery but in no case later than one hour after discovery of the incident, OCSS will report confirmed and suspected incidents to the state agency security contact designated in this security addendum. The requirement for OCSS to report confirmed or suspected incidents to the state agency exists in addition to, not in lieu of, requirements to report to US-CERT or other reporting agencies.

   Policy/Requirements Traceability: OMB Circular A-130 – Appendix I; OMB M-17-12; NIST SP 800-53 Rev 5, IR-6

8. The state agency must prohibit the use of non-state agency furnished equipment to access NDNH information without specific written authorization from the appropriate state agency representatives.

OCSS does not permit personnel to access the agency input files remotely using non-agency furnished equipment.

Policy/Requirements Traceability: NIST SP 800-53 Rev 5, AC-20(1)(2)

9. The state agency must require that personnel accessing NDNH information remotely (for example, telecommuting) adhere to all the security and privacy safeguarding requirements provided in this security addendum. State agency and non-state agency furnished equipment must have appropriate software with the latest updates to protect against attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Before electronic connection to state agency resources, the state agency must scan the state agency and non-state agency furnished equipment to ensure compliance with the state agency standards. All remote connections must be through a Network Access Control, and all data in transit between the remote location and the agency must be encrypted using Federal Information Processing Standards (FIPS) 140-3 encryption standards. Personally owned devices must not be authorized. See numbers 8 and 19 of this section for additional information.

   OCSS does not permit personnel to access the agency input files remotely using non-agency furnished equipment.

   Policy/Requirements Traceability: OMB-M-17-12; NIST SP 800-53 Rev 5, AC-17, AC-20

10. The state agency must implement an effective continuous monitoring strategy and program that must ensure the continued effectiveness of security controls by maintaining ongoing awareness of information security, vulnerabilities, and threats to the information system housing NDNH information. The continuous monitoring program must include configuration management, patch management, vulnerability management, risk assessments before making changes to the system and environment, ongoing security control assessments, and reports to state agency officials as required.

    OCSS has implemented a continuous monitoring strategy and program that ensures the continued effectiveness of security controls by maintaining ongoing awareness of information security, vulnerabilities, and threats to the information system housing the input files. The continuous monitoring program includes configuration management, patch management, vulnerability management, risk assessments before making changes to the system and environment, ongoing security control assessments, and reports to the U.S. Department of Health and Human Services officials as required.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, CA-7(1)(4); NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

11. The state agency must maintain an asset inventory of all software and hardware components within the boundary of the information system housing NDNH information. The inventory must be detailed enough for the state agency to track and report.

    OCSS maintains an inventory of all software and hardware components within the boundary of the information system housing the agency input files.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, CM-2(3)(7), CM-7(1)(2)(4), CM-8(1)(3), CM-11, IA-3, PM-5, SA-4(1)(2)(9)(10), SC-17, SC-18, SI-4(2)(4)(5)

12. The state agency must maintain a system security plan describing the security requirements for the system housing NDNH information and the security controls in place or planned for meeting those requirements. The system security plan must describe the responsibilities and expected behavior of all individuals who access the system.

    OCSS maintains a system security plan that describes the security requirements for the information system housing the agency input files and the security controls in place or planned for meeting those requirements. The system security plan includes responsibilities and expected behavior of all individuals who access the system.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, PL-2; NIST SP 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*

13. The state agency must maintain a plan of action and milestones (corrective action plan) for the information system housing NDNH information to document plans to correct weaknesses identified during security control assessments and to reduce or eliminate known vulnerabilities in the system. The state agency must update the corrective action plan as necessary based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

    OCSS maintains a plan of action and milestones for the information system housing the agency input files to document plans to correct weaknesses identified during security control assessments and to reduce or eliminate known vulnerabilities in the system. OCSS updates the plan of action and milestones as necessary based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, CA-5; NIST SP 800-18 Rev 1

14. The state agency must maintain a baseline configuration of the system housing NDNH information. The baseline configuration must include information on system components (for example, standard software packages installed on workstations,

notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture.

OCSS maintains a baseline configuration of the information system housing the agency input files.

Policy/Requirements Traceability: NIST SP 800-53 Rev 5, CA-7, CA-9, CM-2(3)(7), CM-3(2), CM-5, CM-6, CM-7(1)(2)(4), CM-8(1)(3), CM-11, SI-4(2)(4)(5)

15. The state agency must limit and control logical and physical access to NDNH information to only those personnel authorized for such access based on their official duties, and identified in the records maintained by the state agency pursuant to numbers 6 and 27 of this section. The state agency must prevent personnel from browsing by using technical controls or other compensating controls.

    OCSS limits and controls logical and physical access to the agency input files to only those personnel authorized for such access based on their official duties. OCSS prevents browsing using technical controls that limit and monitor access to the agency input files.

    Policy/Requirements Traceability: 5 U.S.C. § 552a; NIST SP 800-53 Rev 5, AC-2, AC-3

16. The state agency must transmit and store all NDNH information provided pursuant to this agreement in a manner that safeguards the information and prohibits unauthorized access. All electronic state agency transmissions of information must be encrypted utilizing a FIPS 140-3 compliant product.

    OCSS and state agency exchange data via a mutually approved and secured data transfer method that utilizes a FIPS 140-2 compliant product.

    Policy/Requirements Traceability: OMB M-17-12; FIPS 140-2, *Security Requirements for Cryptographic Modules*; NIST SP 800-53 Rev 5, MP-4, SC-8

17. The state agency must transfer and store NDNH information only on state agency owned portable digital media and mobile computing and communications devices that are encrypted at the disk or device level, using a FIPS 140-2 compliant product. See numbers 8 and 18 of this section for additional information.

    OCSS does not copy the agency input files to mobile media.

    Policy/Requirements Traceability: OMB M-17-12; FIPS 140-2

18. The state agency must prohibit the use of computing resources resident in commercial or public facilities (for example, hotels, convention centers, airports) from accessing, transmitting, or storing NDNH information.

    OCSS prohibits the use of computing resources resident in commercial or public facilities (for example, hotels, convention centers, airports) from accessing, transmitting, or storing the agency input files.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, AC-19(5), CM-8(3)

19. The state agency must prohibit remote access to NDNH information, except via a secure and encrypted (FIPS 140-3 compliant) transmission link and using two-factor authentication. The state agency must control remote access through a limited number of managed access control points.

    OCSS prohibits remote access to the agency input files except via a secure and encrypted (FIPS 140-3 compliant) transmission link and using two-factor authentication.

    Policy/Requirements Traceability: OMB M-17-12; FIPS 140-2; NIST SP 800-53 Rev 5, AC-17, IA-2(6)(12), SC-8

20. The state agency must maintain a fully automated audit trail system with audit records that, at a minimum, collect data associated with each query transaction to its initiator, capture date and time of system events and types of events. The audit trail system must protect data and the audit tool from addition, modification or deletion and should be regularly reviewed and analyzed for indications of inappropriate or unusual activity.

    OCSS maintains a fully automated audit trail system with audit records that, at a minimum, collect data associated with each query transaction with its initiator, capture date and time of system events and types of events. The audit trail system must protect data and the audit tool from addition, modification or deletion and should be regularly reviewed and analyzed for indications of inappropriate or unusual activity.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, AU-2, AU-3, AU-6(1)(3), AU-8, AU-9(4), AU-11

21. The state agency must log each computer-readable data extract (secondary store or files with duplicate NDNH information) from any database holding NDNH information and verify that each extract has been erased within 60 days after completing authorized use. If the state agency requires the extract for longer than 60 days to accomplish a purpose authorized pursuant to this agreement, the state agency must request permission, in writing, to keep the extract for a defined period of time,

subject to OCSS written approval. The state agency must comply with the retention and disposition requirements in the agreement.

OCSS does not extract information from the agency input files.

Policy/Requirements Traceability: OMB M-17-12, NIST SP 800-53 Rev 5, MP-4, MP-6, SI-12

22. The state agency must utilize a time-out function for remote access and mobile devices that require a user to re-authenticate after no more than 30 minutes of inactivity. See numbers 8, 9, and 19 of this section for additional information.

    OCSS utilizes a time-out function for remote access and mobile devices that requires a user to re-authenticate after no more than 30 minutes of inactivity.

    Policy/Requirements Traceability: OMB M-17-12, NIST SP 800-53 Rev 5, AC-11, AC-12, AC-17, SC-10

23. The state agency must erase electronic records after completing authorized use in accordance with the retention and disposition requirements in the agreement. (*See* Disposition of Matched Items in section VI of the computer matching agreement). When storage media are disposed of, the media will be destroyed or sanitized so that the erased records are not recoverable.

    OCSS erases the electronic records after completing authorized use in accordance with the retention and disposition requirements in the agreement.

    Policy/Requirements Traceability: 5 U.S.C. § 552a, NIST SP 800-53 Rev 5, MP-4, MP-6, SI-12

24. The state agency must implement a Network Access Control (also known as Network Admission Control (NAC)) solution in conjunction with a Virtual Private Network (VPN) option to enforce security policy compliance on all state agency and non-state agency remote devices that attempt to gain access to, or use, NDNH information. The state agency must use a NAC solution to authenticate, authorize, evaluate, and remediate remote wired and wireless users before they can access the network. The implemented NAC solution must evaluate whether remote machines are compliant with security policies through host(s) integrity tests against predefined templates, such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the state agency enterprise environment. The state agency must disable functionality that allows automatic code execution. The solution must enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the state network and resources while maintaining an audit record on users' access and presence on the state network. See numbers 8 and 19 of this section for additional information.

OCSS ensures that personnel do not access the agency input files remotely using non-agency furnished equipment.

Policy/Requirements Traceability: NIST SP 800-53 Rev 5, AC-17, AC-20, IA-2(6)(12), IA-3

25. The state agency must ensure that the organization responsible for the data processing facility storing, transmitting, or processing NDNH information complies with the security requirements established in this security addendum. The "data processing facility" includes the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information, and the information systems of the state agency including, but not limited to, employees and contractors working with the data processing facility, statewide centralized data centers, contractor data centers, and any other individual or entity collecting, storing, transmitting, or processing NDNH information.

    OCSS ensures that the data processing facility complies with the security requirements established in this security addendum.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, SA-9(2)

26. The state agency must store all NDNH information provided pursuant to this agreement in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

    OCSS stores the agency input files provided pursuant to this agreement in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, PE-2, PE-3

27. The state agency must maintain a list of personnel authorized to access facilities and systems processing sensitive data, including NDNH information. The state agency must control access to facilities and systems wherever NDNH information is processed. Designated officials must review and approve the access list and authorization credentials initially and periodically thereafter, but no less often than annually.

    OCSS maintains lists of personnel authorized to access facilities and systems processing the agency input files. OCSS controls access to facilities and systems wherever the agency input files are processed. Designated officials review and approve the access list and authorization credentials initially and periodically thereafter, but no less often than annually.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, AC-2, PE-2

28. The state agency must label printed reports containing NDNH information to denote the level of sensitivity of the information and limitations on distribution. The state agency must maintain printed reports in a locked container when not in use and must not transport NDNH information off state agency premises. In accordance with the retention and disposition requirements in the agreement, the state agency must destroy these printed reports by burning or shredding.

    OCSS does not generate printed reports containing the agency input files.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, MP-2, MP-3, MP-4, MP-5, MP-6

29. The state agency must use locks and other protective measures at all physical access points (including designated entry and exit points) to prevent unauthorized access to computer and support areas containing NDNH information.

    OCSS uses locks and other protective measures at all physical access points (including designated entry and exit points) to prevent unauthorized access to computer and support areas.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 5, PE-3

IV. CLOUD SOLUTION (OPTIONAL)

The state agency may choose to use cloud computing to distribute services over broader architectures. The state agency must leverage vendors and services only when all FPLS information physically resides in systems located within the United States and all support and services of the system that may facilitate FPLS access must be done from the U.S., its possessions, and territories.

The cloud service provider must be Federal Risk and Authorization Management Program (FedRAMP) certified in order to meet federal security requirements for cloud-based computing or data storage solutions. Cloud implementations are defined by the service model and deployment model used. Software as a Service, Platform as a Service, and Infrastructure as a Service are examples of cloud service models for cloud implementation. The deployment models may include private cloud, community cloud, public cloud, and hybrid cloud. Data security requirements as defined below still must be met regardless of the type of cloud implementation chosen.

1. The cloud-based solution must reside on a FedRAMP compliant system. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

2. Use of a cloud solution must be approved in advance by OCSS at least 45 days before connectivity to FPLS information and confidential child support program information can

be established. States that have already established a cloud solution housing FPLS information must send official notification of this major change to OCSS.

3. FPLS information must be encrypted in transit, to, from, and within the cloud environment. All mechanisms used to encrypt FPLS information must use FIPS 140 validated modules. Adequate logging controls must be in place to determine key changes and access.

4. The state agency must provide the physical address of the cloud provider/data center where FPLS information will be received, processed, stored, accessed, protected and/or transmitted.

5. Software and/or services that receive, transmit, process, or store FPLS information, must be isolated within the cloud environment, so other cloud customers sharing physical or virtual space cannot access other customers information or applications,

6. Any storage devices where FPLS information has resided, must be securely sanitized and/or destroyed using methods acceptable by the National Institute of Standards and Technology (NIST).

7. The state agency must implement sufficient multifactor authentication for accessing their cloud environment including cloud management console(s) and systems within the cloud environment.

8. The state agency and the cloud service provider must comply with all requirements in this agreement, including the security addendum, including the data retention policies agreed upon by the state agency and OCSS to ensure that all required statutory requirements are met. The state agency must ensure such compliance by the cloud service provider.

9. The data stored by the cloud service provider should ONLY be used for the authorized purpose of the matching program.

10. It is the obligation of the state agency to ensure that the cloud solution that houses the FPLS information and confidential child support program information is stored domestically and is specified in the contract or Service Level Agreement between the state agency and the cloud service provider.

V. BREACH REPORTING AND NOTIFICATION RESPONSIBILITY

Upon disclosure of NDNH information from OCSS to the state agency, the state agency is the responsible party in the event of a confirmed or suspected breach of the information, including responsibility for any costs associated with breach mitigation and remediation. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state agency must report confirmed and suspected incidents, in either electronic or physical form, to the security team. Incident reporting contact information is in this security addendum (*See* section VIII). The state agency is responsible for all reporting and notification activities, including but

not limited to: investigating the incident; communicating with required state government breach response officials; notifying individuals whose information is breached; notifying any third parties, including the media; notifying any other public and private sector agencies involved; responding to inquiries about the breach; resolving all issues surrounding the information breach; performing any follow-up activities; correcting the vulnerability that allowed the breach; and any other activity, as required by OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and other federal law and guidance..

Policy/Requirements Traceability: *US-CERT Federal Incident Notification Guidelines* (April 1, 2017); OMB Circular A-130 – Appendix I; OMB M-17-12; NIST SP 800-53 Rev 5, IR-6

VI. SECURITY REQUIREMENTS

1. Security Posture

The state agency has submitted to OCSS the required documentation and OCSS has reviewed and approved the state agency's security posture.

2. Independent Security Assessment

The state agency must submit to OCSS a copy of a recent independent security assessment every four years. Refer to the *Office of Child Support Services Division of Federal Systems Security Requirements for State Agencies Receiving National Directory of New Hires Data*, section VI, for additional guidance.

If major organizational or system framework changes are required after OCSS approves the state's independent security assessment, it is vital for the state to notify OCSS of the changes before implementing them. The state will also need to provide an independent security assessment of the major system changes to OCSS before the system can be approved to access the NDNH.

VII. AUDIT REQUIREMENTS

OCSS has the right to audit the state agency or make other provisions to ensure that the state agency is maintaining adequate safeguards to protect NDNH information. Audits ensure that the security policies, practices and procedures, and controls required by OCSS are in place within the state agency.

Policy/Requirements Traceability: *OMB M-25-04, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements,* January 15,2025; OMB Circular No. A-130 – Appendix I

VIII. PERSONS TO CONTACT

A. The U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Services contact is:

Venkata Kondapolu, Director
Division of Federal Systems
Office of Child Support Services
Administration for Children and Families
Mary E. Switzer Building
330 C Street, SW
Washington, DC 20201
Phone: 202-260-4712
Email: Venkata.kondapolu@acf.hhs.gov

B. Incident Reporting contact information for the U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Services is:

Venkata Kondapolu
Phone: 202-401-9389, option #3
Email: ocsssecurity@acf.hhs.gov

C. The state agency contact is:

[NAME]
[TITLE]
[DIVISION]
[AGENCY]
[MAILING ADDRESS]
[CITY, STATE, ZIP CODE]
Phone: [XXX-XXX-XXXX]
Email: [EMAIL ADDRESS]

IX. APPROVALS

By their signatures below, the authorized officials approve this security addendum.

A. U.S. Department of Health and Human Services Officials

Venkata Kondapolu Director Division of Federal Systems	**Date**
Linda Boyer Deputy Commissioner	**Date**

B. State Agency Official[s]

NAME OF STATE AGENCY

_____

[Name of State Agency Authorized Official] [Title of State Agency Authorized Official]	**Date**
[Name of State Agency Authorized Official (if two signatures are required)] [Title of State Agency Authorized Official]	**Date**

APPENDIX A

Previous Computer Matching Agreements between OCSS and State TANF Agencies

Previous matching agreements and renewals between the Office of Child Support Services (OCSS) and the state agencies administering the Temporary Assistance for Needy Families (TANF) Program are as follows:

- Computer Matching Agreement, HHS No. 2206, effective January 19, 2023 through July 18, 2024; Renewal, effective July 19, 2024 through July 18, 2025.
- Computer Matching Agreement, HHS No. 2002, effective July 19, 2020 through January 18, 2022; Renewal, effective January 19, 2022 through January 18, 2023.
- Computer Matching Agreement, HHS No. 1707, effective January 19, 2018 through July 18, 2019; Renewal, effective July 19, 2019 through July 18, 2020.
- Computer Matching Agreement, HHS No.1505, effective July 13, 2015 through January 12, 2017; Amendment and Renewal, effective January 13, 2017 through January 12, 2018.
- Computer Matching Agreement, HHS No.1205, effective January 13, 2013 through July 12, 2014; Amendment and Renewal, effective July 13, 2014 through July 12, 2015.
- Computer Matching Agreement, HHS No. 1001, effective July 13, 2010 through January 12, 2012; Amendment and Renewal, effective January 13, 2012 through January 12, 2013.
- Computer Matching Agreement, No. 0704, effective January 13, 2008 through July 12, 2009; Renewal, effective July 13, 2009 through July 12, 2010.
- Computer Matching Agreement, No. 0504, effective July 1, 2005 through December 31, 2006; Renewal, effective January 1, 2007 through December 31, 2007.

APPENDIX B

Verification of State TANF Eligibility

Cost-Benefit Analysis

BACKGROUND

State agencies administering the Temporary Assistance for Needy Families (TANF) program voluntarily participate in a computer matching program to access wage and employment information in the National Directory of New Hires (NDNH), which is maintained by the federal Office of Child Support Services (OCSS). The purpose of the computer matching program is to help state TANF agencies with establishing or verifying an individual's eligibility for TANF assistance, to reduce agency payment errors and maintain program integrity, including determining whether duplicate participation exists.

In federal fiscal year 2023, eight state TANF agencies participated in the TANF-NDNH computer matching program to compare TANF applicant and recipient information to employment and wage information maintained in the NDNH. All eight of these state TANF agencies matched to the NDNH at least one time and five of the participating state agencies provided performance outcomes showing cost savings that are attributable to the NDNH.

COSTS

Key Elements 1 and 2: Personnel and Computer Costs

For Agencies –

- **Source Agency:** The cost for OCSS to operate and maintain the NDNH is estimated to be $10.9 million. This includes system enhancements and technical assistance, contracting costs, telecommunications, security, data quality, and software and hardware costs.
- **Non-Federal Agencies:** State TANF agencies are not required to provide OCSS with their personnel and computer processing costs associated with the TANF-NDNH match. However, the state TANF agencies are required to reimburse OCSS for the costs to provide the NDNH information. OCSS calculates fees for each state agency receiving NDNH information. For the five states that submitted performance reports, the combined cost to participate in the TANF-NDNH computer matching program for federal fiscal year 2023 was $237,838.

  Individual State Agency Costs:

  Arizona – Arizona paid $4,355 to match approximately 21,293 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2023.

Maryland – Maryland paid $117,441 to match approximately 186,487 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2023.
Mississippi – Mississippi paid $11,077 to match approximately 9,625 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2023.
New York – New York paid $98,015 to match approximately 672,722 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2023.
Utah – Utah paid $6,950 to match approximately 18,238 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2023.

- **Justice Agencies:** N/A

For clients: N/A
For Third Parties: N/A
For the General Public: N/A

BENEFITS

Key Element 3: Avoidance of Future Improper Payments

To Agencies -

- **Source Agency:** N/A.
- **Non-Federal Agencies:** After verification of previously unknown earnings, state TANF agencies collectively reported cases that were either closed or benefits were reduced. The five TANF agencies collectively avoided approximately $358,119 in improper payments to TANF recipients with previously unknown earnings. The avoided costs resulting from case closures and benefit reductions are attributed to employment and wage information derived from the TANF-NDNH computer matching program.

  Based on the current performance outcome reports, the cost to state TANF agencies to participate in the TANF-NDNH computer matching program is likely outweighed by the benefit of avoiding improper payments. The actual cost avoidance may be even higher than reported because the report includes only the first month avoided costs. It is likely that several TANF recipients whose earnings were discovered through the match would have received an incorrect benefit amount over multiple months had the state not used the NDNH.

  Individual State Agency Benefits:

  Arizona – Arizona matched 12 times and reported 422 cases closed due to earnings, and 72 cases with benefits reduced. Arizona reported $91,349 in unduplicated first month avoided TANF costs.
  Maryland – Maryland matched 12 times and reported 20, cases closed due to earnings, and 24 cases with benefits reduced. Maryland reported $19,466 in unduplicated first month avoided TANF costs.
  Mississippi – Mississippi matched 12 times and reported 285 cases closed due to earnings, and 30 cases with benefits reduced. Mississippi reported $72,374 in unduplicated first month avoided TANF costs.

New York – New York matched 12 times and reported 72 cases closed due to earnings, and 151 cases with benefits reduced. New York reported $80,430 in unduplicated first month avoided TANF costs.

Utah– Utah matched 12 times and reported 105 cases closed due to earnings, and 440 cases with benefits reduced. Utah reported $94,500 in unduplicated first month avoided TANF costs.

- **Justice Agencies:** N/A

To Clients: N/A

To Third Parties: N/A

To the General Public: Improper payments and overpayments avoided through this computer matching program will contribute to improving public confidence in the program and use of federal taxes.

Key Element 4: Recovery of Improper Payments

- **Source Agency:** N/A.
- **Non-Federal Agencies:** States are not required to report recovered funds to OCSS; however, using the NDNH will help state TANF agencies recover improperly paid funds.
- **Justice Agencies:** N/A

For clients: N/A

For Third Parties: N/A

For the General Public: Recovering improper payments as a result of computer matching program will benefit taxpayers.