COMPUTER MATCHING AGREEMENT

BETWEEN

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

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 # 2002

I. PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

This computer matching agreement, hereinafter "agreement," governs a matching program between the U.S Department of Health and Human Services, Administration for Children and Families, Office of Child Support Enforcement (OCSE) and the state agency administering the Temporary Assistance for Needy Families (TANF) program, hereinafter "state agency." This is a standard agreement between OCSE and all state agencies participating in the matching program. The state agency is the "non-federal agency" and OCSE is the "source agency," as defined by the Privacy Act. 5 U.S.C. § 552a(a)(10) and (11). OCSE and participating state agencies have entered into matching agreements and renewals since 2005, the latest of which expires July 18, 2020. (*See* Appendix B of this agreement.) The agreement includes a security addendum and a cost-benefit analysis (*See* Appendix A of this agreement).

A. Purpose of the Matching Program

The Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, hereinafter "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 assist the state agency in establishing or verifying the eligibility for benefits under the TANF program. OCSE shall provide the state agency with new hire, quarterly wage, and unemployment insurance information from the National Directory of New Hires (NDNH) pertaining to individuals who are adult applicants for, or recipients of, assistance 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.

B. Legal Authority

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

> 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 shall 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 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 services with respect to,
    A. cash or in-kind assistance or payments under federal benefit programs, or
    B. recouping payments or delinquent debts under such federal benefit programs. . .
(5) "Non-federal agency" means any state or local government, or agency thereof, 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 thereof, 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, but not limited to, his education, financial transactions, medical history, and criminal or employment history, and that contains his 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 contained in this agreement are defined as follows:

(11) “Federal Parent Locator Service” means a service, which includes the NDNH, conducted under the direction of OCSE pursuant to section 453 of the Social Security Act for purposes specified in sections 453 and 463. 42 U.S.C. §§ 653 and 663.
(12) “National Directory of New Hires (NDNH)” means an automated directory maintained in the Federal Parent Locator Service, established by subsection 453(i)(1) of the Social Security Act, containing new hire, unemployment insurance, 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. 42 U.S.C. §§ 653(i)(l), 653a(b)(1)(C), and (g)(2).
(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. 42 U.S.C. §§ 653a(b)(1)(C) and (g)(2)(A), and 653(i)(1).
(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. 42 U.S.C. §§ 653a(g)(2)(B), 653(i)(1) and (n);
(15) “Unemployment insurance 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. 42 U.S.C. §§ 653a(g)(2)(B) and 653(e)(3) and (i)(1).
(16) “Adult” means an individual who is not a minor child, 42 U.S.C. § 619.
(17) “TANF recipient” means an individual receiving federal Temporary Assistance for Needy Families assistance, as defined in 45 C.F.R. § 260.31.

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

The Privacy Act provides that a Data Integrity Board (DIB) shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective. Unless statutorily excepted or waived by the DIB, a cost benefit analysis must be completed and submitted to the DIB and must demonstrate that the program is likely to be cost effective, or the DIB cannot approve the matching agreement. 5 U.S.C. § 552a(u)(4)(A).

Eight state agencies participated in the federal fiscal year 2019 matching program and provided performance outcomes reports to the Office of Family Assistance. The current Cost-Benefit Analysis (*See* Appendix A) is derived from the fees paid by, and cost savings calculations from, the states' performance outcomes reports. The combined cost of the eight state agencies to access the NDNH is significantly less than the combined savings they identified from the first month in which applicant or recipients' information was compared to information in the NDNH.

B. Other Supporting Justification

The Improper Payments Information Act of 2002, Pub. L. 107-300, the Improper Payments Elimination and Recovery Act of 2010, Pub. L. 111-204, and the Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. 112-248, require federal agencies to identify programs susceptible to significant improper payments and to report to Congress on efforts to reduce such payments. The Office of Management and Budget issued implementing guidance to federal agencies in Appendix C to Circular A-123, *Requirements for Effective Estimation and Remediation of Improper Payments*, (June 26, 2018).

The NDNH is a centralized database of wage and employment information and, as such, provides an effective and efficient means to obtain income information, preferable to other means of obtaining the same information. The matching program will assist the state agency in detecting fraud, waste and abuse and will enhance program integrity by strengthening the state agency's oversight and management of the program. It will serve as a deterrent to some individuals who otherwise may fraudulently apply for and receive TANF benefits, and it will provide information to reduce erroneous payments, which is consistent with requirements of the Improper Payments Information Act , subsequent legislation, and guidance The matching program will also provide 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 that is not readily available through the State Directory of New Hires, state workforce agencies, or other data reporting systems. The matching 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 positive results of the previous matching programs between the state agency and OCSE further justify the proposed matching program. *See* section II.C and Appendix A of this agreement.

C. Specific Estimate of Any Savings

In federal fiscal year 2020, the Office of Family Assistance conducted the cost-benefit analysis based on information provided by state agencies from the NDNH match outcomes pertaining to federal fiscal year 2018. *See* Appendix A. After verification of previously unknown earnings, state agencies collectively reported 6,607 cases that were either closed or benefits were reduced and collectively avoided approximately $1.1 million in costs. The cost-benefit analysis demonstrates that the matching program is likely to be cost effective and will likely continue to help states reduce benefit payments.

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. Systems of Records

1. OCSE.

The NDNH contains new hire, quarterly wage, and unemployment insurance information furnished by state and federal agencies and is maintained by OCSE in the system of records, titled "OCSE National Directory of New Hires," No. 09-80-0381, last published in full at 80 FR 17906 (April 2, 2015) and partially revised at 83 FR 6591 (Feb.14, 2018). The disclosure of NDNH records by OCSE to the state agency constitutes a "routine use," as defined by the Privacy Act. 5 U.S.C. § 552a(b)(3). Routine use (8) of the system of records authorizes the disclosure of NDNH records to the state agency. 80 FR 17906, 17907 (April 2, 2015).

2. State Records

The state agency records used in the information comparison contain information collected by the state agency in its administration of the TANF program. States are authorized to collect such information pursuant to subsections 1137(a) and (b)(1) of the Social Security Act (42 U.S.C. § 1320b-7(a)(1) and (b)[(1)), which require an applicant for, or recipient of, TANF benefits to furnish a Social Security number as a condition of eligibility. .

B. Number of Records Involved

The combined caseload of all state TANF programs is approximately 491,216 adult TANF applicants and recipients. The input file provided to OCSE 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 OCSE by the state agency.

The approximate number of records in the output file provided to the state agency by OCSE depends 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 OCSE contains records pertaining to individuals who are adult TANF applicants for, or recipients of, TANF benefits. Each individual record contains the following data elements, where available:

- Submitting state code (two-digit FIPS code)
- Date stamp (input file transmission date)
- TANF caseload month and year of adult TANF applicants and recipients
- Adult TANF applicant/recipient Social Security number
- Adult TANF applicant/recipient's first, middle, and last name

OPTIONAL:

- Passback data (state agency information used to identify individuals within the input file to be returned on the output file)
- Same state data indicator (indicates whether the state agency requests NDNH new hire, quarterly wage, or unemployment insurance even if the information was provided by that same state)

To enhance the accuracy of records used in the matching program and fairness to the individuals to whom the records pertain, the name and Social Security number combinations contained in the state agency input file are verified using Social

Security Administration processes. Such verification increases the likelihood that NDNH information provided to the state agency pertains to the appropriate individuals.

2. NDNH Data Elements

To accomplish the purposes 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 OCSE will contain the requested NDNH new hire, quarterly wage, and unemployment insurance information, if any, pertaining to the individuals whose Social Security numbers are contained in the state agency input file. The file will also contain a code indicating whether the state requested OCSE to verify the name and Social Security number combination of each individual and a code indicating why a record was rejected.

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 (42 U.S.C. § 653(j)(3)) requires a comparison and disclosure to assist States to carry out their responsibilities under state TANF programs to the extent and with the frequency that the Secretary determines to be effective.

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 the TANF program. The state agency requests comparisons and disclosures at the following frequencies: on a monthly basis for comparison against the new hire file; and on a quarterly basis, the comparison will also include quarterly wage and unemployment insurance files.

E. Projected Start and Completion Dates

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

- OCSE and the authorized state agency officials sign the agreement;
- The state agency submits the documentation required by OCSE to assess the security posture of the state agency; and
- OCSE completes the notice and reporting requirements specified in subsection XII.A of the agreement.

The projected start date of this agreement is July 19, 2020 and the projected expiration date is January 18, 2022 (18 months from the start date), or January 18, 2023 (if the agreement is renewed for another year).

IV. NOTICE PROCEDURES

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

The Privacy Act requires that the matching agreement shall specify procedures for providing individualized notice at the time of application, and notice 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, upon annual recertification or reexamination that the information provided by applicants and recipients may be verified through matching programs. Methods for notification 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 renewal; 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 a 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).

OCSE will publish the notice of the matching program in the *Federal Register*.at least 30 days before conducting the program and will make the notice and this agreement available on the HHS computer matching agreement internet site; these publications will provide constructive notice of the matching program to affected individuals. OCSE will not publish the *Federal Register* notice until OCSE 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*.

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, as required by § 552a(p).

A. Verification Procedures

The Privacy Act requires that each matching agreement specify procedures for verifying information produced in the matching program and an opportunity to contest findings, as required by subsection (p). 5 U.S.C. § 552a(o)(1)(E). 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;
> > . . .
> > (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, pursuant to the Privacy Act, the state agency understands that information obtained from the NDNH is not conclusive evidence of the address and employment information of an identified individual and 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 calling 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.

Information in the NDNH is also verified to ensure accuracy of records (*See* section IX). Records in an NDNH output file from OCSE to a state agency will indicate whether each name and Social security number combination in the match results obtained from the NDNH has been verified for accuracy. OCSE verification procedures and output file indicators increase the likelihood that the NDNH information OCSE provides to the state agency will pertain to the appropriate individuals.

B. Opportunity to Contest Findings

The state agency has established and implemented procedures which require that, prior to taking adverse action against an individual, the state agency must notify the individual of the findings and of the opportunity to contest the findings, including the date by which the individual must respond to the notice, in accordance with 5 U.S.C. § 552a(p)(1).

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 OCSE, which includes the information contained in those records, even NDNH records that are not labeled as such. Electronic files and information and any paper printouts shall be disposed of as provided in the security addendum at III. 23. and 28.

A. State Agency Records in the Input File

OCSE may retain the records contained in the input file provided to OCSE 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 OCSE.

B. NDNH Records in the Output File

1. Copy of NDNH Records in the Output File

OCSE may retain copies of the records contained in the NDNH output file provided to the state agency by OCSE 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 the Output File Provided to State Agency

The state agency may retain NDNH records contained in the output file provided to the agency by OCSE 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 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. Office of Management and Budget Memorandum 01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, Security Controls. (December 20, 2000).

In accordance with the Privacy Act and OMB guidance, OCSE sets forth procedures and controls to ensure the appropriate equivalent level of security for records matched and the results of such programs. Such procedures and controls 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 the 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).

Subsection 453(j)(3) of the Social Security Act, under which this matching program is authorized, further restricts the redisclosure and use of records. Subsections 453(j)[(3)(A) and (B) of the Social Security Act provide that OCSE shall disclose to the state agency information in the NDNH only to the extent that OCSE determines that the disclosure would not interfere with the effective operation of the child support program. 42 U.S.C. § 653(j)(3)(A) and (B). OCSE may not commence, or may discontinue, disclosure of NDNH information upon a determination that such disclosure interferes with the effective operation of the child support program. OCSE will provide the state agency with ten days advance written notice prior to discontinuation of the disclosure of NDNH information.

In accordance with such requirements, OCSE shall use state agency records solely as provided in this agreement and shall not duplicate or redisclose those records within or outside of OCSE. The state agency shall 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.

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 of this agreement), the state agency must obtain OCSE's written approval prior to any redisclosure. The state agency shall submit a written request to OCSE describing the purpose, manner, and frequency of the proposed redisclosure and the entities to which such redisclosure is to be made. The state agency shall certify that it will ensure the appropriate equivalent level of security controls on the entity's use of NDNH information. OCSE shall 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 OCSE by state and federal agencies. OCSE verifies the accuracy of name and Social Security number combinations maintained by OCSE 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 Social Security number combination has a corresponding name and Social Security number combination within Social Security Administration databases.

One hundred percent of the employee name and Social Security number combinations contained in the new hire file and the unemployment insurance file against which input files are compared have been verified against Social Security Administration databases.

For quarterly wage, 77 percent of name and Social Security number 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

Pursuant to OCSE's procedure to verify state agency records prior to conducting an information comparison with the NDNH (*See* section III.C.1), name and Social Security number 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 in order to monitor or verify compliance with this agreement. 5 U.S.C. § 552a(o)(1)(K). OCSE 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 of the U.S. Department of Health and Human Services 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).

OCSE 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 shall

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 shall reimburse OCSE in accordance with the terms of such reimbursement agreement.

XII. DURATION OF AGREEMENT

A. Effective Date of the Agreement

The State Agency and OCSE intend that the effective date of this agreement will be July 19, 2020, the day after the expiration date of the renewal of the prior matching agreement, No. 1707.

This agreement will not be effective until the agreement is approved by the HHS Data Integrity Board and has been fully signed, OCSE has reported the proposal to re-establish this matching program to the Congressional committees of jurisdiction and to OMB in accordance with 5 U.S.C. § 552a(o)(2)(A) and (r) and OMB Circular A-108, and, after completion of OMB's review, OCSE has published notice of the matching program in the *Federal Register* for 30 days in accordance with 5 U.S.C. § 552a(e)(12) and OMB Circular A-108.

The U.S. Department of Health and Human Services will post a copy of the published notice and this agreement to its computer matching agreement internet site and will provide a copy of the notice to the state agency.

This agreement shall remain in effect for 18 months. The parties may, within 3 months prior to the expiration date of this agreement, renew the agreement for a period of up to one year if the matching program will be conducted without any change and OCSE and the state agency certify to the HHS Data Integrity Board in writing that the program has been conducted in compliance with the agreement. 5 U.S.C. § 552a(o)(2)(D).

Subsection (q) provides 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)(A) and (B).

B. Modification of the Agreement

This agreement may be modified at any time by a written amendment to the agreement which is approved by the state agency and OCSE. The proposed modification must be reviewed by HHS DIB counsel to determine if the change is significant and requires a new agreement.

C. Termination of the Agreement

This agreement may be terminated at any time with the consent of both agencies.

Either agency may unilaterally terminate this agreement upon written notice to the other agency, in which case the termination date shall 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 OCSE has reason to believe that the verification and opportunity to contest requirements of subsection (p) of the Privacy Act (as amended) or any other requirement of this agreement is not being met, OCSE shall terminate disclosures of records contained in the NDNH under the agreement, in accordance with subsection 552a(q)(1) of the Privacy Act (as amended). 5 U.S.C. § 552a(q)(1).

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

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

XIII. PERIODIC REPORTING OF PERFORMANCE OUTCOMES

The Office of Management and Budget requires OCSE to periodically report measures of the performance of the Federal Parent Locator Service, 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. OCSE is required to provide performance measures demonstrating how the Federal Parent Locator Service supports OCSE's strategic mission, goals and objectives, and cross-agency collaboration. OCSE also requests such performance reporting to ensure matching partners use NDNH information for the authorized purpose.

To assist OCSE 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 shall provide OCSE with performance outputs and outcomes attributable to its use of NDNH information for the purposes set forth in this agreement.

The state agency shall annually provide such reports, in a format determined by OCSE and approved by the Office of Management and Budget in accordance with the Paperwork Reduction Act, to OCSE, no later than three months after the end of each fiscal year of the matching program

The performance reports may also assist the Office of Family Assistance on behalf of the state agency in the development of a cost-benefit analysis of the matching program required for any subsequent matching agreements in accordance with 5 U.S.C. § 552a(o)(1)(B). *See* section II.A of this agreement and Appendix A.

XIV. PERSONS TO CONTACT

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

Maureen Henriksen
Data Access Manager
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
Mary E. Switzer Building
330 C Street SW, 5th Floor
Washington, DC 20201
Phone: 202-205-3848
Email: maureen.henriksen@acf.hhs.gov

B. The state agency contacts 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]

XV. APPROVALS

By their signatures below, the authorized officials approve this agreement.

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

/s/	
Scott M. Lekan Commissioner, Office of Child Support Enforcement	**Date** 1/27/2020

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

/s/	
Scott W. Rowell Chairperson	**Date** 3/16/2020

C. State Agency Official

NAME OF STATE AGENCY

_____

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

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

SECURITY ADDENDUM

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

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 Enforcement (OCSE) and the state agency administering the Temporary Assistance For Needy Families (TANF) (state agency) shall 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, OCSE and the state agency agree to comply with the security requirements established by the U.S. Department of Health and Human Services and OCSE. OCSE 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 OCSE.

OCSE 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, OCSE shall provide the state agency with written notification of such changes and require written assurance by the state agency that it shall 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 OCSE and the state agency, and entities specified in the agreement which are hereinafter “OCSE” and “state agency.”

III. SECURITY AND PRIVACY SAFEGUARDING REQUIREMENTS

The state agency shall comply with the *Office of Child Support Enforcement Division of Federal Systems Security Requirements for State Agencies Receiving National Directory of New Hires Data*. The state agency received this document on November 1, 2018. The safeguarding requirements in this security addendum are drawn from this document.

This section provides the safeguarding requirements with which OCSE and the state agency shall comply and continuously monitor. The state agency shall 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 OCSE for protecting the agency input files are as follows:

1. The state agency shall 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.

   OCSE 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 4, AC-3, AC-6

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

   OCSE 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* PL-4(1), PS-6, PS-8

3. The state agency shall 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).

OCSE 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 4, PL-4(1), PS-6, PS-8

4. The state agency shall 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 shall 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 shall receive security and privacy awareness training before accessing NDNH information and at least annually thereafter. The training shall 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.

   OCSE 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 4, AT-2(2), AT-3

5. The state agency personnel with authorized access to NDNH information shall 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 shall 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.

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

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 4, PS-6

6. The state agency shall maintain records of authorized personnel with access to NDNH information. The records shall 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 shall make such records available to OCSE upon request.

   OCSE 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 4, AT-4

7. The state agency shall 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 shall report confirmed and suspected incidents, in either electronic or physical form, to OCSE, as designated in this security addendum. The requirement for the state agency to report confirmed or suspected incidents involving NDNH information to OCSE exists in addition to, not in lieu of, any state agency requirements to report to the United States Computer Emergency Readiness Team (US-CERT).

   OCSE 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, OCSE will report confirmed and suspected incidents to the state agency security contact designated in this security addendum. The requirement for OCSE 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 4, IR-6

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

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

Policy/Requirements Traceability: NIST SP 800-53 Rev 4, AC-20(1)(2)

9. The state agency shall 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 shall 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 shall scan the state agency and non-state agency furnished equipment to ensure compliance with the state agency standards. All remote connections shall be through a Network Access Control (NAC) solution, and all data in transit between the remote location and the agency shall be encrypted using Federal Information Processing Standards (FIPS) 140-2 encryption standards. Personally owned devices shall not be authorized. See numbers 8 and 19 of this section for additional information.

   OCSE 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 4, AC-17, AC-20

10. The state agency shall implement an effective continuous monitoring strategy and program that shall 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 shall 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.

    OCSE 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 4, CA-7(1); NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

11. The state agency shall maintain an asset inventory of all software and hardware components within the boundary of the information system housing NDNH

information. The inventory shall be detailed enough for the state agency to track and report.

OCSE 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 4, CM-2(1)(3)(7), CM-7(1)(2)(4), CM-8(1)(3)(5), CM-11, IA-3, SA-4(1)(2)(9)(10), SC-17, SC-18, SI-4(2)(4)(5), PM-5

12. The state agency shall 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 shall describe the responsibilities and expected behavior of all individuals who access the system.

    OCSE 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 4, PL-2(3); NIST SP 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*

13. The state agency shall 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 shall update the corrective action plan as necessary based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

    OCSE 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. OCSE 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 4, CA-5; NIST SP 800-18 Rev 1

14. The state agency shall maintain a baseline configuration of the system housing NDNH information. The baseline configuration shall 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.

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

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

15. The state agency shall 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 shall prevent personnel from browsing by using technical controls or other compensating controls.

    OCSE 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. OCSE 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 4, AC-2, AC-3

16. The state agency shall 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 shall be encrypted using a FIPS 140-2 compliant product.

    OCSE and state agency exchange data via a mutually approved and secured data transfer method that uses 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 4, MP-4, SC-8

17. The state agency shall 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.

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

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

18. The state agency shall 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.

    OCSE 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 4, AC-19(5), CM-8(3)

19. The state agency shall prohibit remote access to NDNH information, except via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication. The state agency shall control remote access through a limited number of managed access control points.

    OCSE prohibits remote access to the agency input files except via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication.

    Policy/Requirements Traceability: OMB M-17-12; FIPS 140-2; NIST SP 800-53 Rev 4, AC-17, IA-2(11)(12), SC-8

20. The state agency shall 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 shall 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.

    OCSE 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 shall 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 4, AU-2, AU-3, AU-6(1)(3), AU-8, AU-9(4), AU-11

21. The state agency shall 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 90 days after completing required use. If the state agency requires the extract for longer than 90 days to accomplish a purpose authorized pursuant to this agreement, the state agency shall request permission, in writing, to keep the extract for a defined period of time,

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

OCSE does not extract information from the agency input files.

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

22. The state agency shall use 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.

    OCSE uses 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 4, AC-11, AC-12, AC-17, SC-10

23. The state agency shall erase electronic records from its storage media after completing authorized use in accordance with the retention and disposition requirements in the computer matching 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.

    OCSE 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 4, MP-4, MP-6, SI-12

24. The state agency shall implement a 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 shall 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 shall 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 shall disable functionality that allows automatic code execution. The solution shall 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.

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

Policy/Requirements Traceability: NIST SP 800-53 Rev 4, AC-17, AC-20, IA-2(11)(12), IA-3

25. The state agency shall 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.

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

    Policy/Requirements Traceability: NIST SP 800-53 Rev 4, SA-9(2)

26. The state agency shall 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.

    OCSE 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 4, PE-2, PE-3

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

    OCSE maintains lists of personnel authorized to access facilities and systems processing the agency input files. OCSE 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 4, AC-2, PE-2

28. The state agency shall label printed reports containing NDNH information to denote the level of sensitivity of the information and limitations on distribution. The state agency shall maintain printed reports in a locked container when not in use and shall not transport NDNH information off state agency premises. In accordance with the retention and disposition requirements in the agreement (*See* Disposition of Matched Items in section VI of computer matching agreement), the state agency shall destroy these printed reports by burning or by shredding with a cross-cut shredder.

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

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

29. The state agency shall 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.

    OCSE 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 4, PE-3

IV. CLOUD SOLUTION (OPTIONAL)

The state agency may choose to use cloud computing to distribute services over broader architectures. 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 OCSE before connectivity to NDNH information can be established.

3. The state agency and the cloud service provider must comply with all requirements in this agreement, including the security addendum, in accordance with section VIII of the agreement, including the data retention policies agreed upon by the state agency

and OCSE to ensure that all required statutory requirements are met. The state agency must ensure such compliance by the cloud service provider.

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

5. It is the obligation of the matching partner to ensure that the cloud housing NDNH information is stored domestically and is specified in the contract or Service Level Agreement between the matching partner and the cloud service provider.

V. BREACH REPORTING AND NOTIFICATION RESPONSIBILITY

Upon disclosure of NDNH information from OCSE 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 shall report confirmed and suspected incidents, in either electronic or physical form, to OCSE, as designated in this security addendum. 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 4, IR-6

VI. SECURITY REQUIREMENTS

1. Security Posture

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

2. Independent Security Assessment

The state agency shall submit to OCSE a copy of a recent independent security assessment every four years. Refer to the *Office of Child Support Enforcement 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 OCSE approves the state's independent security assessment, it is vital for the state to notify OCSE of the changes before implementing them. The state will also need to provide an independent security assessment of the major system changes to OCSE before the system can be approved to access the NDNH.

VII. AUDIT REQUIREMENTS

OCSE 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 OCSE are in place within the state agency.

Policy/Requirements Traceability: OMB M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements,* November 19, 2019; 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 Enforcement security contact is:

Venkata Kondapolu, Acting Director
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
Mary E. Switzer Building
330 C Street, SW, 5th Floor
Washington, DC 20201
Phone: 202-260-4712
Fax: 202-401-5558
E-mail: Venkata.kondapolu@acf.hhs.gov

B. The state agency security 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

/s/	
Venkata Kondapolu Acting Director Division of Federal Systems Office of Child Support Enforcement	**Date** 1/23/2020
/s/	
Scott M. Lekan Commissioner, Office of Child Support Enforcement	**Date** 1/27/2020

B. State Agency Official[s]

NAME OF STATE AGENCY

_____

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

APPENDIX A

COST BENEFIT ANALYSIS
FOR
VERIFICATION OF STATE TANF ELIGIBILITY

BACKGROUND

State agencies administering the Temporary Assistance for Needy Families (TANF) program can 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 Enforcement (OCSE). 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 2018, eight state TANF agencies implemented 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 six 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 OCSE to operate and maintain the NDNH is estimated to be $5.5 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 OCSE with their personnel and computer processing costs associated with the TANF-NDNH match. However, the state TANF agencies are required to reimburse OCSE for the costs to provide the NDNH information. OCSE calculates fees for each state agency receiving NDNH information. The combined cost for all eight states to participate in the TANF-NDNH computer matching program for federal fiscal year 2018 was $241,863.

  Individual State Agency Costs:

  Illinois – Illinois paid $18,686 to match approximately 193,803 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2018.
  Maryland – Maryland paid $51,322 to match approximately 191,849 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2018.

Montana – Montana paid $7,070 to match approximately 154,999 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2018.
New York – New York paid $88,426 to match approximately 706,337 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2018.
Pennsylvania – Pennsylvania paid $52,578 to match approximately 675,426 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2018.
Utah – Utah paid $8,440 to match approximately 54,279 records pertaining to applicants for or recipients of TANF benefits during federal fiscal year 2018.

- **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 six TANF agencies collectively avoided approximately $ $1,058,525 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. While the report includes only the first month avoided cost, it is likely that several TANF recipients whose earnings were discovered through the match would have received an incorrect benefit amount for longer than a single month had the state not used the NDNH. In addition, this estimate does not include cost avoidance attributable to other programs that would also be affected by the discovery of unreported employment.

Individual State Agency Benefits:

Illinois – Illinois matched 9 times and reported 628 cases closed due to earnings, and 470 cases with benefits reduced. Illinois reported $257,704 in unduplicated first-month avoided TANF costs.

Maryland – Maryland matched 9 times and reported 1,052 cases closed due to earnings, and 298 cases with benefits reduced. Maryland reported $207,996 in unduplicated first-month avoided TANF costs.

Montana - Montana matched 11 times and reported 2,613 cases closed due to earnings, and 91 cases with benefits reduced. Montana reported $27,561 in unduplicated first-month avoided TANF costs.

New York – New York matched 12 times and reported 117 cases closed due to earnings, and 320 cases with benefits reduced. New York reported $149,952 in unduplicated first-month avoided TANF costs.

Pennsylvania – Pennsylvania matched 12 times and reported 310 cases closed due to earnings, and 348 cases with benefits reduced. Pennsylvania reported $201,879 in unduplicated first-month avoided TANF costs.

Utah – Utah matched 12 times and reported 182 cases closed due to earnings, and 1,078 cases with benefits reduced. Utah reported $213,433 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 OCSE; 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.

APPENDIX B

Previous Computer Matching Agreements between OCSE and State TANF Agencies

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

- 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.