

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
UNEMPLOYMENT COMPENSATION PROGRAM**

“Administration of Unemployment Compensation Program”

HHS DIB #1504

Reference

- Computer Matching Agreement, HHS Data Integrity Board Approval No. 1204 effective January 13, 2013 through July 12, 2014; Amendment and Renewal, effective July 13, 2014 through July 12, 2015.
- Computer Matching Agreement, HHS Data Integrity Board Approval No. 1002, effective July 13, 2010 through January 12, 2012; Amendment and Renewal, effective January 13, 2012 through January 12, 2013.
- Computer Matching Agreement, HHS Data Integrity Board Approval No. 0705, effective January 13, 2008 through July 12, 2009; Renewal, effective July 13, 2009 through July 12, 2010.
- Computer Matching Agreement, HHS Data Integrity Board Approval No. 0505, effective July 1, 2005 through December 31, 2006; Renewal, effective January 1, 2007 through December 31, 2007.

I. PURPOSE AND LEGAL AUTHORITY FOR CONDUCTING THE MATCHING PROGRAM; DEFINITIONS

This computer matching agreement, hereinafter “agreement,” governs a matching program between the federal Office of Child Support Enforcement (OCSE) and the state agency administering the unemployment compensation (UC) program (state agency).

A. Purpose and Legal Authority for Conducting 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 primary purpose of the matching program is to assist the state agency in administering the UC benefits program under federal or state law.

42 U.S.C. §653(j)(8)(A). Subsection 303(a)(1) of the Social Security Act requires the state agency to ensure the timely and accurate payment of UC benefits to qualified workers “when due” in accordance with state laws. 42 U.S.C. §503(a)(1). To fulfill this statutory responsibility, state agencies are principally organized by benefit and tax functions to pay benefits and to assess and collect unemployment tax contributions. Program integrity activities are an important component to both benefit and tax functions.

OCSE will provide state agencies with new hire and quarterly wage information from the National Directory of New Hires (NDNH) pertaining to applicants for, or recipients of, UC benefits, unless pursuant to section 453(j)(8)(B), the Secretary determines that the disclosure would interfere with the effective operation of the child support program under this part D , title IV of the Act. 42 U.S.C. §653(j)(8)(B). The state agency will use NDNH comparison results to establish or verify the eligibility of, or continuing compliance with, statutory and regulatory requirements by applicants for, or recipients of, UC benefits. In the performance of its benefit function, the state agency may transmit to OCSE the name and SSN of a UC applicant or beneficiary and OCSE may disclose to the state agency information on such individuals and their employers maintained in the NDNH to:

- Verify wages paid to applicants and beneficiaries to determine initial and continuing eligibility for benefits;
- Prevent, detect, and collect improper UC benefit payments by identifying beneficiaries who have returned to work and fraudulently continue to claim benefits, or identifying beneficiaries who have unreported wages; and
- Locate individuals with outstanding UC overpayments or “skip-tracing.”

In support of administering tax compliance function, the state agency may also use NDNH comparison results to locate employers and to collect delinquent UC tax contributions from employers, and to identify employers who have failed to report new hires or employee wages, or misclassified the employees as independent contractors.

The state agency may also use information in the NDNH to meet federal operational and performance reporting requirements such as:

- To assist the state agency in obtaining data on the reemployment of beneficiaries for the Employment and Training Administration 9047 report. *See* Unemployment Insurance Program Letter No. 1-06, Change 1, issued August 2, 2006 by U.S. Department of Labor (DOL), Employment and Training Administration.

- To obtain information on selected UC claims for investigation as part of the state agency's Benefit Accuracy Measurement (BAM) Program, for purposes of quality control and meeting Improper Payment Information Act reporting requirements. BAM is a statistical survey of paid and denied UC claims which assesses the accuracy of UC payments and denials of claims by conducting comprehensive audits of representative samples of payments and denied claims. BAM matches information about claimants receiving benefits with information in the NDNH in order to identify claimants who have returned to work but continue to claim UC.
- To provide data for ad hoc benefits and tax reports that may be required from time to time for special federal or state initiatives which are necessary for the effective and efficient administration of the state UC program.

Subsection 453(j)(8) of the Social Security Act provides the legal authority for conducting the matching program. In pertinent part, subsection 453(j)(8)(A) states as follows:

If, for purposes of administering an unemployment compensation program under Federal or State law, a State agency responsible for the administration of such program transmits to the Secretary the names and social security account numbers of individuals, the Secretary shall disclose to such State agency information on such individuals and their employers maintained in the National Directory of New Hires, subject to this paragraph

42 U.S.C. §653(j)(8)(A).

B. Background

Records contained in a system of records may not be disclosed to a recipient agency or non-federal agency for use in a "matching program," as defined by the Privacy Act, except pursuant to a written agreement containing certain provisions as specified in subsection 552a(o) of the Privacy Act, 5 U.S.C. §552a(o). This agreement contains the specified provisions. It also contains, or incorporates by reference, requirements from the Social Security Act, pursuant to which the matching program is authorized, and other federal privacy and security requirements governing the disclosure of personally identifiable information. OCSE is the "source agency" and the state agency is the "non-federal agency," as defined by the Privacy Act.

In addition, the Social Security Act provides that a state agency requesting information under paragraph 453(j)(8)(D) shall adhere to uniform procedures established by the Secretary governing information requests and data matching under such paragraph. 42 U.S.C. §653(j)(8)(D).

This is a standard agreement between OCSE and all state agencies participating in the NDNH data match. The agreement sets forth the terms and conditions of a new matching program, and includes a security addendum and a cost-benefit analysis

(Appendix A). A reimbursement agreement (not attached or appended) will be executed each fiscal year of the agreement in accordance with section XI of this agreement.

OCSE and participating state agencies have entered into matching agreements and renewals since 2005, the latest of which expires on July 12, 2015.

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):

- (2) "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;
- (3) "maintain" includes maintain, collect, use, or disseminate;
- (4) "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 contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph;
- (5) "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;

- (7) "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;
- (8) "matching program" --
 - (A) means any computerized comparison of --
 - (i) two or more automated systems of records or a system of records with non-federal records for the purpose of --
 - (I) 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, cash or in-kind assistance or payments under federal benefit programs, or
 - (II) recouping payments or delinquent debts under such federal benefit programs;

- (10) "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;
- (11) "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;
- (12) "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;

Additional terms contained in this agreement are defined as follows:

- (1) "Benefit Accuracy Measurement (BAM) Program" means the quality control program for UC established in 20 CFR Part 602. BAM is a statistical survey designed to estimate the accuracy of UC paid and denied claims through audits of representative samples of these claims;
- (2) "Benefit Payment Control (BPC)" means the primary administrative activity conducted by the state agency to identify and establish for recovery fraud and non-fraud UC payments;
- (3) "reemployment" means the match of the SSN of an individual who has received a first payment of UC during a calendar quarter with the SSN of the same individual included in the report of wages submitted by an employer during the subsequent calendar quarter;
- (4) "ETA 227 Report" means the Employment and Training Administration 227 Overpayment Detection and Recovery Activities Report (OMB No. 1205-0187, OMB Expiration Date: 8/31/2017). This is a quarterly report submitted by the state agency to report the results of its BPC activities;
- (5) "benefit year earnings (BYE) overpayment" means the overpayments that are caused by unreported or erroneously reported benefit year earnings. For example, when an individual fails to correctly report earnings for the same week(s) for which UC benefits are paid;
- (6) "new hire information" means information pertaining to newly hired employees reported to the NDNH by state and federal agencies pursuant to sections 453A(g)(2)(A), 453A(b)(1)(C) and 453(i)(1) of the Social Security Act, 42 U.S.C. §§653a(g)(2)(A), 653a(b)(1)(C) and 653(i)(1);

- (8) "quarterly wage information" means employee wage information reported to the NDNH by state and federal agencies pursuant to sections 453A(g)(2)(B), 453(i)(1) and 453(n) of the Social Security Act, 42 U.S.C. §§653a(g)(2)(B), 653(i)(1) and 653(n).

II. JUSTIFICATION FOR THE MATCHING PROGRAM AND ANTICIPATED RESULTS

The Privacy Act requires that each matching agreement specify the justification for the matching program and the anticipated results, including a specific estimate of any savings.

5 U.S.C. §552a(o)(1)(B). In pertinent part, the Privacy Act also provides that “a Data Integrity Board 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.” 5 U.S.C. §552a(u)(4)(A).

A. Justification for the Matching Program

State agencies are authorized under 453(j)(8) of the Social Security Act to conduct an information comparison with the NDNH. 42 U.S.C. §653(j)(8). Identifying employment status and wages of unemployment compensation applicants and recipients improves program integrity by strengthening the state agency’s oversight and management of the program. State agencies first participated in a computer matching program in 2005. The positive results of state agencies using NDNH information pursuant to the previous matching program further justify the matching program. *See* section II.B of this agreement and the Cost-Benefit Analysis located in Appendix A of this agreement

The NDNH provides useful information of applicants for and recipients of UC benefits as well as employer compliance with UC tax contributions, including information that is not readily available through the State Directory of New Hires, state workforce agencies or other data reporting systems. In particular, the NDNH affords state agencies information on individuals who are employed with the federal government and those who are employed in another state. The NDNH includes individuals who have been rehired by a previous employer after having been previously separated from such prior employment for at least 60 days (Pub. L 112-40, section 253, effective April 12, 2012, amending subsection 453A(a)(2) of the Social Security Act, 42 U.S.C. § 653a(a)(2)). The comparison and disclosure under the matching program may serve as a deterrent to some individuals who otherwise may fraudulently apply for and receive UC benefits, and will encourage employers to comply with UC tax contributions and to report on and categorize new hires properly.

Studies done by DOL confirm that use of NDNH results in earlier detection of improper payments, thus preventing future overpayments and increasing the likelihood of overpayment recovery. DOL mandated use of the NDNH for the BAM program in 2007 (See UIPL No. 3-07, Change 1) and to detect BYE overpayments beginning in December 2011 (See UIPL No. 19-11). The mandatory use of NDNH is based on the Department’s administrative authority granted under Section 303(a)(1) of the Social Security Act and Sections 3306(h) and 3304(a)(4) of the Internal Revenue Code.

B. Anticipated Results

As of December 2014, 54 states have matched unemployment compensation claims data

with the NDNH. For the period of CY 2012, states identified \$165.3 million in overpayments through NDNH and SDNH matching. Based on historical data of state agency use of SDNH data, access to the NDNH has increased the amount of overpayment detections by 55 percent and increased the proportion of all overpayments detected through new hire matching by 49.1 percent. These figures are calculated based on the pre-NDNH CY 2004 baseline of \$71.38 million detected using SDNH, which is 6.3 percent of all overpayments detected and established.

III. DESCRIPTION OF THE RECORDS; FREQUENCY; METHOD OF TRANSMISSION; AND PROJECTED STARTING AND COMPLETION DATES

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. OCSE System of Records and State Agency Records

The NDNH contains new hire, quarterly wage, and unemployment insurance information furnished by state and federal agencies and is maintained by OCSE in its system of records "OCSE National Directory of New Hires," No. 09-80-0381, published in the *Federal Register* at 80 FR 17906 on April 2, 2015. The disclosure of NDNH information 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 (13) of the system of records authorizes the disclosure of NDNH information to the state agency. 80 FR 17906, 17907 (April 2, 2015).

The state agency records used in the information comparison contain information collected by the state agency in its administration of the UC program. States are authorized to collect such information pursuant to subsections 1137(a)(1) and (b)(3) of the Social Security Act, which require an applicant or recipient to furnish a Social Security number as a condition of eligibility for certain programs. 42 U.S.C. §§1320b-7(a)(1) and (b)(3).

B. Specified Data Elements Used in the Matching Program

1. Data Elements in the State Agency Input File; Approximate Number of Records

The state agency input file contains records pertaining to individuals who are applicants for, or recipients of, UC benefits. Each individual record contains the following data elements, where available:

- Name
- SSN

Additionally, the state agency shall indicate in the Passback Data field of the Input Detail Records a code to identify the purpose for which the record is being submitted for NDNH matching. For the purpose of the BAM program, the state agency shall comply with guidance issued by DOL. *See* UIPL No. 3-07, Change 1 "Use of National Directory of New Hires in Unemployment Insurance (UI) Benefit Accuracy Measurement (BAM) Audits," February 27, 2008.

For records submitted to OCSE for the purpose of obtaining reemployment data for the ETA 9047 report, the state agency shall include the appropriate code in the

Passback Data field and designate the quarterly wage reporting quarters to be matched, as specified in UIPL No. 1-06, Change 1.

For the purpose of obtaining new hire data for the BAM program, UIPL No. 3-07 instructed state BAM units to coordinate with the organizational unit responsible for their state agency's administration of NDNH matching. Each state agency will identify a unique code in the Passback Data field to identify BAM records submitted for NDNH matching.

The combined caseload of all regular UC programs includes approximately 2.5 million UC recipients. The input file provided to OCSE by the state agency will contain records representing a portion of that caseload. *See* Section XVI.C of this agreement for the estimated number of records to be submitted to OCSE by the state agency.

2. Verification of Name and Social Security Number Combinations

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 NDNH and the state agency records contained in the 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.

3. State Agency and NDNH Data Elements Used to Conduct the Comparison

OCSE will compare Social Security numbers provided by the state agency, and verified by either the state agency before the match or by OCSE when the input file is submitted, to Social Security numbers in the NDNH.

4. NDNH Data Elements Requested by the State Agency

To accomplish the purpose of this matching program, the state agency requests the following data elements from the new hire and quarterly wage files:

a) New Hire File

- Date new hire file processed by OCSE
- Employee name
- Employee address
- Employee date of hire
- Employee state of hire
- Federal Employer Identification Number (FEIN)
- State Employer Identification Number (EIN)
- Department of Defense status code
- Employer name
- Employer address

b) Quarterly Wage File

- Date quarterly wage record processed by OCSE
- Employee name
- Quarterly wage processed date
- Federal Employer Identification Number (FEIN)
- State Employer Identification Number (EIN)
- Department of Defense status code
- Employer name
- Employer address
- Employee wage amount
- Quarterly wage reporting period

5. Data Elements from the NDNH Contained in the Output File Provided to the State Agency and Approximate Number of Records

The output file provided to the state agency by OCSE will contain NDNH new hire and quarterly wage information pertaining to the individuals whose records are contained in the state agency input file. The output file will also contain a code indicating whether the name and Social Security number combination of each individual was verified.

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.

Match results pertaining to records submitted for the ETA 9047 reemployment report will be identified by a code in the Passback Data field, as specified in UIPL No. 1-06, Change 1.

C. Frequency of Information Comparisons

The Secretary has determined that comparisons and disclosures at a frequency established by the state agency are effective in assisting states to carry out their responsibilities under the UC program. The state agency requests comparisons and disclosures on a weekly basis against new hire and quarterly wage files.

D. Method of Transmission

Input files from the state agency to OCSE and output files from OCSE to the state agency will be transmitted via a managed file transfer method that utilizes Federal Information Processing Standards 140-2.

E. Projected Starting 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 official sign the agreement
- The state agency submits an Independent Security Assessment for OCSE to assess the security posture of the state agency
- OCSE satisfies the notice and reporting requirements, specified in section XII.A of the agreement

The projected expiration date of the agreement shall be 18 months from the effective date referenced in section XII.A.

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 notice periodically thereafter as directed by the Data Integrity Board of the U.S. Department of Health and Human Services, subject to guidance provided by the Director of the federal Office of Management and Budget, to applicants for and recipients of financial assistance or payments under federal benefit programs that any information they provide 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, that the information provided by applicants and recipients may be verified through matching programs. Such procedures are in accordance with directions by the

Data Integrity Board of the U.S. Department of Health and Human Services, subject to guidance by the federal Office of Management and Budget.

B. Publishing General Notice of Matching Program in the *Federal Register*

The Privacy Act requires agencies to publish notice of the establishment or revision of a matching program in the *Federal Register* at least 30 days prior to conducting such program. 5 U.S.C. §552a(e)(12).

At least 30 days prior to conducting the matching program, OCSE will publish the notice of the matching program in the *Federal Register*. The notice will clearly identify the system of records, categories of records, and purposes for which the records will be used.

C. Furnishing Report of Matching Program and Agreement to Congress and the Federal Office of Management and Budget

The Privacy Act requires that a copy of each matching agreement shall be transmitted to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform, and be available upon request to the public, in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals. 5 U.S.C. §552a(r) and 552a(o)(2)(A). Agencies are also required to provide a report of a matching program, including the agreement, to the federal Office of Management and Budget. *See* Federal Office of Management and Budget Circular No. A-130, Appendix 1, 4(d).

OCSE will provide a report of the matching program, including a copy of this agreement, to the appropriate congressional committees and the federal Office of Management and Budget, and will make the agreement available to the public upon request.

V. VERIFYING INFORMATION AND OPPORTUNITY TO CONTEST FINDINGS

A. Requirements for Verifying Information and Opportunity to Contest Findings

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)(1),(2) and (3).

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 federal Office of Management and Budget's guidelines at 54 FR 25818 (June 19, 1989).

B. Procedures for Verifying Information and Opportunity to Contest Findings

The state agency recognizes that information obtained from the NDNH is not conclusive evidence of the address and employment information of an identified individual, but is an indication that further verification is warranted. The state agency has established and implemented procedures for verifying information produced in the

matching program and providing the individual an opportunity to contest findings. Such procedures provide that, before taking adverse action against an individual, the state agency must independently verify the information produced in the matching program; notify the individual of any findings; and inform the individual of the opportunity to contest such findings in accordance with subsections (p)(1) and (2) of the Privacy Act. 5 U.S.C. §§552a(p)(1) and (2).

VI. RETENTION AND DISPOSITION OF RECORDS

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 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).

The following provisions specify the retention periods for the records contained in the input file provided by the state agency and the NDNH records, including the information contained therein, provided to state agency in the matching program, even NDNH records that are not labeled as such. After the retention periods, OCSE and the state agency shall destroy the records in accordance with of the security addendum herein, including the erasure of all electronic records.

A. State Agency Records Contained in the Input File Provided to OCSE

OCSE may retain the records contained in the input file provided 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 Contained in the Output File Provided by OCSE to the State Agency

1. Copy of Records Contained in NDNH Output File

OCSE may retain copies of the records contained in the output file provided 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 files to the state agency.

2. NDNH Records Contained in Output File Provided to the State Agency

The state agency may retain NDNH records only for the period of time required to

achieve the authorized purpose of the matching program, but no longer than three years from the date of disclosure of the information to the state agency.

VII. SECURITY PROCEDURES

The Privacy Act requires that each matching agreement specify procedures for ensuring the 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 Office of Management and Budget 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. RESTRICTIONS ON DUPLICATION; REDISCLOSURE; AND USE OF RECORDS

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 contained 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 must 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)(2) 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).

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 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 the agreement, including the security addendum. The state agency may not redisclose or duplicate the results of the information comparison.

Furthermore, subsection 453(j)(8)(C)(i) provides the state agency may not use or disclose information provided by OCSE except for purposes of administering a UC program under federal or state law. 42 U.S.C. § 653(j)(8)(C)(i). The state agency may use or disclose information provided by OCSE solely for purposes of administering a UC program under federal or state law.

If a state agency determines that redisclosure 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 before 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 redisclosee's use of NDNH information. OCSE shall review any such request and advise the state agency whether the request is approved or denied.

IX. ASSESSMENT OF ACCURACY OF RECORDS

The Privacy Act requires that each matching agreement specify information on assessments that have been made on the accuracy of 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 subsection 453(j)(1) of the Social Security Act. 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 matched have been verified against Social Security Administration databases. For quarterly wage, only 77% of the incoming data has a verified name and SSN combination, since some states and employers do not capture enough name information in their records to complete this process. However, information comparisons may be conducted and reliable results obtained.

B. State Agency Records

Prior to conducting information comparison of NDNH and state agency records, and upon the request of the state agency, OCSE requests verification by the Social Security Administration of the accuracy of name and Social Security number combinations furnished by the state agency to OCSE. Thus, name and Social Security number combinations within state agency records have a high degree of accuracy.

X. ACCESS TO RECORDS BY THE COMPTROLLER GENERAL

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

Subsection 453(k)(3) of the Social Security Act requires a state or federal agency that receives information from the Secretary 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).

Subsection 453(j)(8)(E) of the Social Security Act requires the state agency to reimburse OCSE in accordance with subsection (k)(3), for the costs incurred by OCSE in furnishing the information.. 42 U.S.C. §653(j)(8)(E).

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 fiscal year of the matching program and DOL, on behalf of the state agency, shall reimburse OCSE in accordance with the terms of such reimbursement agreement.

DOL is authorized to use funds appropriated for grants to states under Title III of the Social Security Act for the purpose of reimbursing OCSE on behalf of the state agencies for the services provided to such state agencies pursuant to this matching agreement.

XII. EFFECTIVE DATE; DURATION; MODIFICATION AND TERMINATION OF AGREEMENT

A. Effective Date of the Agreement

The Privacy Act provides that a copy of each matching agreement shall be transmitted to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform. Copies must also be available upon request to the public. 5 U.S.C. §552a(o)(2)(A)(i) and (ii). *See also* notice and reporting requirements in 5 U.S.C. §552a(e)(12) and (r) and the Federal Office of Management and Budget Circular No. A-130, Appendix I, 4(d).

An agreement is not effective until agencies comply with all notice and reporting requirements. Where applicable, agencies may agree upon a later effective date, for example, to coincide with the expiration of a renewal of a previous matching agreement between the agencies. The state agency and OCSE intend that the effective date of this agreement will be July 13, 2015, the day after the expiration date of the amendment and renewal of the matching agreement, HHS DIB Approval No. 1204.

Unless the Federal Office of Management and Budget or Congress disapproves the agreement within 40 days of the date the transmittal letter for the report of matching program was signed, or the Federal Office of Management and Budget grants a waiver of 10 days of the 40-day review period, or public comments are received that result in cancellation or deferral of the implementation of the program, this agreement shall be effective no sooner than the later of the following dates:

- July 13, 2015 (the day after the expiration date of the Amendment and Renewal of the matching agreement, HHS DIB Approval No.1204)
- 30 days after the date the notice of matching program is published in the *Federal Register*
- 40 days after the date OCSE provides a Report of Matching Program to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform under 5 U.S.C. §552a(o)(2)(A) and to the Office of Information and Regulatory Affairs of the federal Office of Management and Budget.

B. Duration of the Agreement

The Privacy Act requires that each matching agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program. 5 U.S.C. §552a(o)(2)(C). This agreement shall remain in effect for 18 months. The Data Integrity Board of the U.S. Department of Health and Human Services may 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 Data Integrity Board in writing that the program has been conducted in compliance with the agreement. 5 U.S.C. §552a(o)(2)(D).

C. Modification of the Agreement

This agreement may be modified at any time by a written amendment which is approved by the state agency, OCSE and the Data Integrity Board of the U.S. Department of Health and Human Services.

D. 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 that this date does not exceed the approved duration of this agreement.

If OCSE has reason to believe that the verification and opportunity to contest requirements of subsection (p) of the Privacy Act or any other requirement of this agreement are not being met, OCSE shall terminate disclosures of records contained in the NDNH under the agreement, in accordance with Subsection 552a(q)(1).
5 U.S.C. §552a(q)(1).

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. COST-BENEFIT ANALYSIS

The Privacy Act provides 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). In pertinent part, the Privacy Act also provides that “a Data Integrity Board 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.” 5 U.S.C. §552a(u)(4)(A).

DOL provided a cost-benefit analysis to OCSE in accordance with the Privacy Act on March 3, 2015, *See* Appendix A.

XIV. PERIODIC REPORTING OF PERFORMANCE OUTCOMES

The federal 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 Federal Office of Management and Budget IT 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.

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 DOL with performance outputs and outcomes attributable to its use of NDNH information for the purposes set forth in this agreement.

DOL will develop such reports and provide them to OCSE on an annual basis, no later than three months after the end of each fiscal year of the matching program.

The performance reports may also assist DOL, 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.B of the agreement.

XV. PERSONS TO CONTACT

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

Linda Boyer, Data Access and Security Manager
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
370 L'Enfant Promenade S.W., 4th Floor
Washington, DC 20447
Telephone: 202-401-5410
Fax: 202-401-5558
E-mail: linda.boyer@acf.hhs.gov

- B.** The state agency contacts are:


NAME AND TITLE
NAME OF AGENCY
ADDRESS OF AGENCY
Telephone:
Fax:
E-mail:

NAME AND TITLE
NAME OF AGENCY
ADDRESS OF AGENCY
Telephone:
Fax:
E-mail:

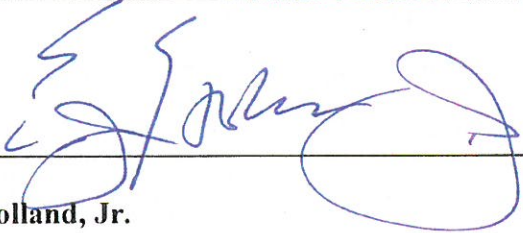
XVI. APPROVALS AND NUMBER OF RECORDSS

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

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

	
Vicki Turetsky Commissioner	Date 4/10/15

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

	
E. J. Holland, Jr. Chairperson	Date 5/14/15

C. 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 Title of State Agency Authorized Official	Date

The NDNH comparison results for the state of _____ will be transmitted to the following address:

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 this agreement.

SECURITY ADDENDUM

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

And

State Agency Administering the Unemployment Compensation Program

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 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 personnel, facilities, documentation, information, electronic and physical records, other machine-readable information, and the information systems of OCSE and the state agency, which are hereinafter referred to as "OCSE" and "state agency."

III. SECURITY AND PRIVACY SAFEGUARD 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 requirements are drawn from this document. The state agency received this document on April 7, 2015.

This section provides the safeguarding requirements with which OCSE and the state agency shall comply. 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 file are as follows:

1. The state agency shall restrict access to, and disclosure of, the NDNH information to authorized personnel who need the 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 file to authorized personnel who need it to perform their official duties as authorized in this agreement.

Policy/Requirements Traceability: Privacy Act 5 USC 552a (b)(1)

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 file to ensure that only authorized personnel have access.

Policy/Requirements Traceability: Privacy Act 5 USC 552a; National Institute of Standards and Technology (NIST) Special Publication (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 the NDNH information, the safeguards required to protect the NDNH information, and the civil and criminal sanctions for non-compliance contained in the applicable federal and state laws, including Section 453(1)(2) of the Social Security Act. 42 U.S.C. § 653(1)(2).

OCSE advises all personnel who will access the agency input file 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: Privacy Act 5 USC 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 and other federal and state 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: Federal Information Security Management Act; Federal Office of Management and Budget (OMB) Circular A-130; OMB M-07-16; 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 the NDNH information 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 file sign non-disclosure agreements and rules of behavior.

Policy/Requirements Traceability: OMB Circular A-130 - Appendix III; OMB M-07-16; NIST SP 800-53 Rev 4, PS-6

6. The state agency shall maintain records of authorized personnel with access to the 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 file. The records contain a copy of each individual's signed non-disclosure agreement, rules

of behavior, or equivalent document and proof of 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 security or privacy incidents (unauthorized disclosure involving personal information), or suspected incidents 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 the Federal Parent Locator Service (FPLS) Information Systems Security Officer (ISSO) designated on section VI.A of 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 any other reporting agencies.

OCSE has appropriate procedures in place to report security or privacy incidents, or suspected incidents involving the agency input file. 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 agency security contact designated on this security addendum. The requirement for OCSE to report confirmed or suspected incidents to the agency exists in addition to, not in lieu of, requirements to report to US-CERT or other reporting agencies.

Policy/Requirements Traceability: OMB Circular A130 – Appendix III; OMB M-07-16; 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 file 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, 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 mobile devices shall not be authorized. See number 8 and number 18 of this section for additional information.

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

Policy/Requirements Traceability: OMB M-06-16, *Protection of Sensitive Agency Information*; OMB-M-07-16; NIST SP 800-53 Rev 4, AC-17, AC-20

10. The state agency shall implement an effective continuous monitoring strategy and program to 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 file. 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 HHS 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 at a level of granularity deemed necessary by the state agency for internal tracking and reporting.

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

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 file 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 file 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, *Guide for Developing Security Plans for Federal Information Systems*

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 file.

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

number 6 and number 27 of this section. The state agency shall prevent personnel from browsing case files not assigned to them by using technical controls or other compensating controls.

OCSE limits and controls logical and physical access to the agency input file 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 file.

Policy/Requirements Traceability: Privacy Act 5 USC 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.

OCSE 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-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 4, MP-4, SC-8

17. The state agency shall prohibit NDNH information from being transferred to and stored on portable digital media and mobile computing and communications devices unless encrypted at the disk or device level, using a FIPS 140-2 compliant product. See number 8 and number 18 of this section for additional information.

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

Policy/Requirements Traceability: OMB M-07-16; FIPS 140-2, *Security Requirements for Cryptographic Modules*

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 file.

Policy/Requirements Traceability: NIST SP 800-53 Rev 4, AC-19(5), CM-8(3)

19. The state agency shall prohibit remote access to the NDNH information, except via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication, as required by OMB M-06-16. The state agency shall control remote access through a limited number of managed access control points. If the state

agency cannot provide two-factor authentication, the state agency shall submit to OCSE a written description of compensating controls, subject to written approval by OCSE before allowing remote access.

OCSE prohibits remote access to the agency input file except via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication as required by OMB M-06-16.

Policy/Requirements Traceability: OMB M-06-16; OMB M-07-16; 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 file 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's 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 file.

Policy/Requirements Traceability: OMB M-06-16; OMB M-07-16

22. The state agency shall 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 18 of this section for additional information.

OCSE 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-06-16; OMB M-07-16

23. The state agency shall erase electronic records after completing authorized use in accordance with the retention and disposition requirements in the agreement.

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

Policy/Requirements Traceability: Privacy Act 5 USC 552a(o)(1)(F)

24. The state agency shall implement a Network Access Control (also known as Network Admission Control (NAC)) solution in conjunction with a 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 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 number 8 and number 18 of this section for additional information.

OCSE ensures that personnel do not access the agency input file 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 the 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's ensures that the data processing facility complies with the security requirements 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 the 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 file 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 file. OCSE controls access to facilities and systems wherever the agency input file is 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. When no longer needed, in accordance with the retention and disposition requirements in the agreement, the state agency shall destroy printed reports by shredding or burning.

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

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. 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 breach or suspected breach of the 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 the FPLS ISSO designated in Section VII.A of 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; communicating with any third parties, including the media, as necessary; notifying any other public and private sector agencies involved; responding to inquiries about the breach; resolving all issues surrounding the breach of NDNH information; performing any necessary follow-up activities to correct the vulnerability that allowed the breach; and any other activities, as required by OCSE.

Policy/Requirements Traceability: OMB Circular A130 – Appendix III; OMB M-06-19; OMB M-07-16; NIST SP 800-53 Rev 4, IR-6

V. SECURITY CERTIFICATION

A. Security Posture

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

B. 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 and/or system framework changes have taken place since the previous independent security assessment, the state agency shall have an independent security assessment conducted within six (6) months of the change. The state agency shall submit the results of the independent assessment to OCSE.

VI. AUDIT REQUIREMENTS

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

Policy/Requirements Traceability: OMB M-11-33; OMB Circular No. A-130, Appendix III.

VII. 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:

Linda Boyer, FPLS Information System Security Officer
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
370 L'Enfant Promenade, S.W., 4th Floor
Washington, DC 20447
Telephone: 202-401-5410
Fax: 202-401-5558
E-mail: linda.boyer@acf.hhs.gov

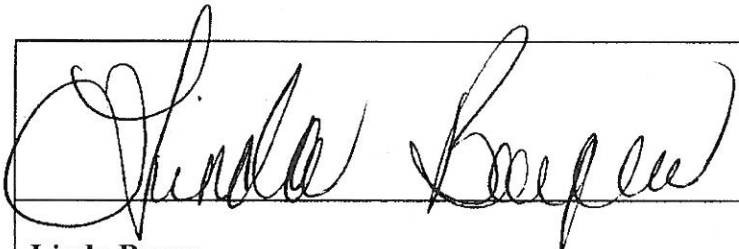

- B.** The state agency security contact is:

[NAME AND TITLE]
[NAME OF AGENCY]
[ADDRESS OF AGENCY]
Telephone:
Fax:
E-mail:

VIII. APPROVALS

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

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

	
Linda Boyer FPLS Information Systems Security Officer	Date 4-8-15
	
Vicki Turetsky Commissioner	Date 4/10/15

B. State Agency Program Official

Name of State Agency Authorized Official Title of State Agency Authorized Official	Date
Name of State Agency Authorized Official Title of State Agency Authorized Official	Date

APPENDIX A

NATIONAL DIRECTORY OF NEW HIRES COST/BENEFIT ANALYSIS FOR UNEMPLOYMENT INSURANCE (UI)

BACKGROUND:

State Agencies cross match unemployment insurance (UI) claim records against State Directory of New Hire (SDNH) databases to identify UI overpayments. Public Law 108–295 (“SUTA Dumping Prevention Act of 2004”) authorized state agencies to access the National Directory of New Hire (NDNH), “for purposes of administering an unemployment compensation program under Federal or state law.” The NDNH provides states further access to information such as multi-state employer, Federal civilian and military data. This supplemental information has yielded a significant increase in the number of overpayments prevented and recovered.

Since states have gained access to the NDNH, the number and amount of overpayments detected through new hire matching (both SDNH and NDNH) have increased most years:

Calendar Year (CY)	Total \$ Amount SDNH and/or NDNH
CY 2004	\$71,382,827
CY 2005	\$78,537,515
CY 2006	\$98,431,185
CY 2007	\$122,858,207
CY 2008	\$141,667,995
CY 2009	\$158,014,864
CY 2010	\$147,531,359
CY 2011	\$162,533,639
CY 2012	\$165,318,674
CY 2013	\$146,460,391
CY2014	\$139,182,698

*Data does not include Emergency Unemployment Compensation overpayments identified by crossmatches.

BENEFIT ANALYSIS:

As of December 2014, 54 states have matched UI claims data with the NDNH. For the period January 2004 to December 2014 states identified \$ 1.432 billion in overpayments through NDNH and SDNH matching. Since 2006, the first year in which overpayments detected through NDNH matching were reported, states identified an average of \$142.4 million more in overpayments per year. The Department of Labor (DOL) estimates that use of SDNH and NDNH matching saved approximately \$94.2 million during the calendar year 2014.

Beginning in Calendar Year 2012, DOL began capturing NDNH as a separate line item from SDNH overpayments, in its reports.

CY	Total Amount of NDNH Overpayments	NDNH amount of overpayments as a percent of total new hire overpayments
2013	\$58,642,113	40.04%
2014	\$53,583,820	38.50%

In CY 2014, states reported 38.50% of new hire established overpayments were identified by matching with NDNH.

Since 2008, DOL has required that states submit for NDNH matching paid UI claims selected for audit as part of the Benefit Accuracy Measurement (BAM) survey. In IPIA 2014, BAM detected an estimated \$281.6 million in overpayments using national new hire data.

National Directory of New Hire (W-4) Crossmatch Savings Estimates

Detailed data on UI overpayment detections and recoveries for CY 2013 and 2014 are summarized in the following tables.

CY 2013 Data.

Total Overpayments Established*	\$2.354 B
Total Overpayments Recovered	\$1.491 B
Percent Recovered	63.32%
Overpayments Established Using New Hire	\$146.46 M
Estimated New Hire Overpayments Recovered	\$92.74 M
Estimated Overpayments Prevented By New Hire	\$141.37 M
Total Overpayments Prevented + Recovered**	\$234.10 M

CY 2014 Data

Total Overpayments Established*	\$1.471 B
Total Overpayments Recovered	\$955.9 M
Percent Recovered	64.98%
Overpayments Established Using New Hire	\$139.2 M
Estimated New Hire Overpayments Recovered	\$90.4 M
Estimated Overpayments Prevented By New Hire	\$94.2 M
Total Overpayments Prevented + Recovered**	\$184.6 M