

**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 SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM**

*Information Comparisons and Disclosures to Assist in Administering the  
Supplemental Nutrition Assistance Program*

U.S. Department of Health and Human Services Data Integrity Board #1612

**I. PURPOSE AND LEGAL AUTHORITY FOR CONDUCTING THE MATCHING PROGRAM; 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 Supplemental Nutrition Assistance Program (SNAP) (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 Agriculture Act of 2014, Pub. L. 113-079, amended section 11(e) of the Food and Nutrition Act of 2008, by adding a requirement that the state agency "shall request wage data directly from the National Directory of New Hires established under section 453(i) of the Social Security Act (42 U.S.C. 653(i)) relevant to determining eligibility to receive supplemental nutrition assistance program benefits and determining the correct amount of such benefits." 7 U.S.C. 2020(e)(24).

Consistent with the federal mandate, the purpose of the matching program is to assist the state agency with establishing or verifying the eligibility for assistance under SNAP to reduce payment errors and maintain program integrity, including determining whether duplicate participation exists. 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, and recipients

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

Subsection 453(j)(10) of the Social Security Act provides the legal authority for conducting the matching program as follows:

Information comparisons and disclosure to assist in administration of supplemental nutrition assistance programs.—

(A) In general.—If, for purposes of administering a supplemental nutrition assistance program under the Food and Nutrition Act of 2008, a State Agency responsible for the administration of the program transmits to the Secretary the names and social security account numbers of individuals, the Secretary shall disclose to the State Agency information on the individuals and their employers maintained in the National Directory of New Hires, subject to this paragraph.

(B) Condition on disclosure by the secretary.—The Secretary shall make a disclosure under subparagraph (A) only to the extent that the Secretary determines that the disclosure would not interfere with the effective operation of the program under this part.

(C) Use and disclosure of information by State Agencies.—

(i) In general.—A State Agency may not use or disclose information provided under this paragraph except for purposes of administering a program referred to in subparagraph (A).

(ii) Information security.—The State Agency shall have in effect data security and control policies that the Secretary finds adequate to ensure the security of information obtained under this paragraph and to ensure that access to such information is restricted to authorized persons for purposes of authorized uses and disclosures.

(iii) Penalty for misuse of information.—An officer or employee of the State Agency who fails to comply with this subparagraph shall be subject to the sanctions under subsection (1)(2) to the same extent as if the officer or employee were an officer or employee of the United States.

(D) Procedural requirements.—State Agencies requesting information under this paragraph shall adhere to uniform procedures established by the Secretary governing information requests and data matching under this paragraph.

(E) Reimbursement of costs.—The State Agency shall reimburse the Secretary, in accordance with subsection (k)(3), for the costs incurred by the Secretary in furnishing the information requested under this paragraph.

42 U.S.C. § 653(j)(10).

## **B. Background**

A computerized comparison of records from systems of records for the purpose of administering SNAP constitutes a “matching program” as defined by the Privacy Act. Records contained in a system of records may not be disclosed to a recipient agency or a 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 (as amended). 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, National Institute of Standards and Technology Series 800 Special Publications, U.S. Department of Health and Human Services Information Security Program Policy, Office of Management and Budget guidance, U.S. Department of Health and Human Services and OCSE requirements, 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. 5 U.S.C. §552a(a)(9) and (11).

This is a standard agreement between OCSE and all state agencies participating in the matching program. The agreement includes a security addendum and a cost-benefit analysis (Appendix A). A reimbursement agreement (not attached or appended) shall be executed each federal fiscal year of the computer matching agreement in accordance with section XI of this agreement.

OCSE and participating state agencies have entered into matching agreements and renewals since 2009, the latest of which expires on February 15, 2017. *See* Appendix B of this agreement. This agreement sets forth the terms and conditions of a new matching program.

## **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)(1), 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.

## 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).

### A. Justification for the Matching Program

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*, (October 20, 2014).

The Supplemental Nutrition Assistance Program (SNAP) was reauthorized on February 7, 2014, as part of the Agricultural Act of 2014, P.L. 113-79. States are now required to verify wage data of adult household members through the NDNH, to determine eligibility and the correct amount of SNAP benefits at the time of certification, see 7 U.S.C. 2020(e)(24). State agencies are authorized under 453(j)(10) of the Social Security Act to conduct an information comparison with the NDNH. 42 U.S.C. §653(j)(10).

The matching program will assist the state agency in enhancing 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 SNAP benefits, and it will provide information to reduce erroneous payments. The NDNH provides useful information on the employment and earnings of adult applicants for, and recipients of, SNAP benefits, including information that is not readily available through the State Directory of New Hires or other data reporting systems, 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; and 3) those whose information is not readily available through the State Directory of New Hires, state workforce agencies, or other data reporting systems.

The positive results of state agencies using NDNH information pursuant to the previous matching program further justify the matching program. *See* section II.B and Appendix A of this agreement.

#### **B. Anticipated Results of the Matching Program**

In federal fiscal year 2015, state agencies submitted performance outcomes attributable to the NDNH matching program that indicate over \$21 million in combined first month SNAP costs avoided. *See* Appendix A. The parties to this agreement anticipate that state agencies will obtain similar savings and operation benefits through continued use of the NDNH.

The cost-benefit analysis demonstrates that the cost for state SNAP agencies to participate in the SNAP-NDNH matching program is outweighed by the benefit of avoiding improper payments. The U.S. Department of Agriculture Food and Nutrition Service anticipates that state SNAP agencies will continue to experience savings and operation benefits through continued use of the NDNH.

### **III. DESCRIPTION OF THE RECORDS; FREQUENCY; METHOD OF TRANSMISSION; 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 (15) of the system of records permits 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 SNAP program. States are authorized to collect such information pursuant to subsections 1137(a) and (b)(4) of the Social Security Act, which require an applicant for, or recipient of, SNAP benefits to furnish a Social Security number as a condition of eligibility. 42 U.S.C. §1320b-7(a)(1) and (b)(4).

## **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 provided to OCSE contains records pertaining to individuals who are adult SNAP applicants for, and recipients of, SNAP benefits. Each individual record contains the following data elements, where available:

- Submitting state code (2-digit FIPS code)
- Date stamp (input file transmission date)
- Adult SNAP applicant/recipient Social Security number
- Adult SNAP applicant/recipient's first, middle, and last name
- 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)
- Passback data (state agency information used to identify individuals within the input file to be returned on the output file)
- Name/Social Security number verification request

The combined caseload of all state SNAP programs is approximately 44 million adult SNAP applicants and recipients. The input file provided to OCSE by the state agency will contain records representing a portion of that state's caseload. See section XVII.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 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 Element Used to Conduct the Comparison**

OCSE will compare Social Security numbers provided by the state agency to the Social Security numbers in the NDNH.

### **4. NDNH Data Elements Requested by the State Agency**

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

**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 status 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 status 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
- Benefit amount
- Unemployment insurance reporting period
- Transmitter state code
- Transmitter state name

**5. Data Elements from the NDNH in the Output File; Approximate Number of Records**

In accordance with subsection 453(j)(10) of the Social Security Act, the output



file provided to the state agency by OCSE will contain available NDNH new hire, quarterly wage, and unemployment insurance information, if any, pertaining to the individuals whose records are contained in the state agency input file. 42 U.S.C. §653(j)(10). 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.

### **C. Frequency of Information Comparisons**

Subsection 453(j)(10) of the Social Security Act requires a comparison and disclosure to assist states in carrying out their responsibilities under state SNAP programs to the extent and with the frequency that the Secretary determines to be effective. 42 U.S.C. §653(j)(10).

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 SNAP 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.

### **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 mutually approved and secure data transfer method that uses Federal Information Processing Standards 140-2 encryption standards.

### **E. Projected Starting and Completion Dates**

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

- 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
- OCSE completes 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 of this agreement.

#### IV. NOTICE PROCEDURES

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

The Privacy Act requires that each matching agreement shall 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 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, 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 Office of Management and Budget.

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

The Privacy Act requires federal 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 shall publish the notice of the matching program in the *Federal Register*. The notice shall clearly identify the systems of records and categories of records being used, and state that the matching program is subject to the review period afforded the Office of Management and Budget and Congress.

##### C. Furnishing Report of Matching Program and Agreement to Congress and the 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 (o)(2)(A). Agencies are also required to provide a report of a matching program, including the agreement, to the congressional committees and to the Office of Management and Budget. See federal Office of Management and Budget Circular No. A-130, Appendix I, 4(d).

OCSE shall provide a report of the matching program, including a copy of this agreement, to the congressional committees and the Office of Management and Budget and shall 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).

Further, subsection (q)(1) of the Privacy Act provides that notwithstanding any other provisions 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* Office of Management and Budget 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 prior to taking adverse action against an individual, the state agency shall 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 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 the NDNH records, which includes the information contained in those records, even NDNH records that are not labeled as such, provided to the state agency in the matching program. CD-ROMs containing electronic files and information shall be destroyed by shredding; electronic files and information shall be erased.

After the retention periods, OCSE and the state agency shall destroy the records including the erasure of all electronic records.

**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 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 federal 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 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)(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).

Subsection 453(j)(10) of the Social Security Act, under which this matching program is authorized, further restricts the redisclosure and use of records. Subsections 453(j)(10)(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)(10)(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 10 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. 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 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 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 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**

Prior to conducting an 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 the name and Social Security number combinations furnished to OCSE. Thus, name and Social Security number combinations within the 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 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 of the computer matching agreement, and the state agency shall reimburse OCSE in accordance with the terms of such reimbursement agreement.

## **XII. EFFECTIVE DATE, DURATION, MODIFICATION, AND TERMINATION OF AGREEMENT**

### **A. Effective Date of the Agreement**

The Privacy Act provides that no agreement shall be effective until 30 days after publication of a notice of matching program in the *Federal Register* and the date a copy of the agreement is transmitted to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform. 5 U.S.C. §552a(e)(12) and (o)(2)(B). *Also see* 5 U.S.C. §552a(o)(2)(A) and (r) and Office of Management and Budget Circular No. A-130, *Management of Federal Information Resources*, Appendix I, 4(d) (Nov. 28, 2000).

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 February 16, 2017, the day after the expiration date of the Renewal of the matching agreement, U.S. Department of Health and Human Services Data Integrity Board, No. 1403.

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 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 latest of the following dates:

- February 16, 2017 (the day after the expiration date of the Renewal of the matching agreement, U.S. Department of Health and Human Services Data Integrity Board No. 1403;)
- 30 days after the date the notice of matching program is published in the *Federal Register*;
- 40 days after the date OCSE transmits the report of matching program to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform and to the Office of Management and Budget, Office of Information and Regulatory Affairs.



## **B. Duration of the Agreement**

The Privacy Act requires that a 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).

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).

## **C. 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, OCSE, and by 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 for the 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) of the Privacy Act. 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. COST-BENEFIT ANALYSIS**

The Privacy Act 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).

OCSE shall submit to the Data Integrity Board of the U.S. Department of Health and Human Services the cost-benefit analysis provided by the state agencies.

### **XIV. NECESSITY OF INFORMATION FOR AUTHORIZED PURPOSE**

Subsection 453(j)(10)(C) of the Social Security Act requires the state agency to seek minimum information only to the extent necessary to administer the program described in subsection 453(j)(10)(A). 42 U.S.C. §§653(j)(10)(A)and(C).

The state agency will comply with such requirement by ensuring that each individual pertaining to whom information is requested and each data element requested, the frequency of transmission and the retention and disposition periods of NDNH information are necessary to accomplish the authorized purpose for obtaining NDNH information—determining eligibility and detecting fraud. (See sections III.B, III.D, and VI. of this agreement.)

### **XV. 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 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.

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 performance reports may also assist 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 this agreement.

**XVI. 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  
Mary E. Switzer Building  
330 C Street SW, 5th Floor  
Washington, DC 20201  
Phone: 202-401-5410  
Fax: 202-401-5553  
E-mail: linda.boyer@acf.hhs.gov

- B.** The state agency contacts are:

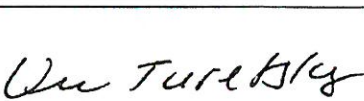
[NAME]  
[TITLE]  
[AGENCY]  
[MAILING ADDRESS]  
[CITY, STATE, ZIP CODE]  
Phone: [XXX-XXX-XXXX]  
Fax: [XXX-XXX-XXXX]  
E-mail: [EMAIL ADDRESS]

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

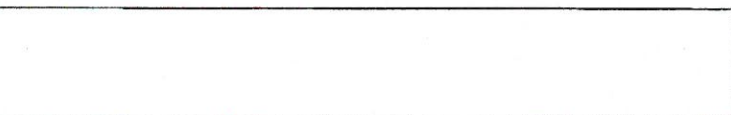

**XVII. APPROVALS; NUMBER OF RECORDS**

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

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

	
<b>Vicki Turetsky</b> Commissioner	<b>Date</b> 8/23/16


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

	
<b>Colleen Barros</b> Chairperson 	<b>Date</b> 11/2/16


**XVII. APPROVALS; NUMBER OF RECORDS**

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

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

	
<b>Vicki Turetsky</b> Commissioner	<b>Date</b> 8/23/16

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

	
<b>Colleen Barros</b> Chairperson	<b>Date</b> 11/8/16

C. State Agency Official[s]

NAME OF STATE AGENCY

\_\_\_\_\_

<b>[Name of State Agency Authorized Official]</b> [Title of State Agency Authorized Official]	<b>Date</b>

<b>[Name of State Agency Authorized Official, if approval by two officials is required]</b> [Title of State Agency Authorized Official]	<b>Date</b>

The NDNH comparison results for the state of \_\_\_\_\_ will be transmitted to the following physical 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 the 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 Supplemental Nutrition Assistance 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 June 24, 2016.

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 U.S.C. 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 U.S.C. 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 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 prior to 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 prior to 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 prior to 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 exist 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. Prior to 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 prior to 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 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 U.S.C. 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 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.

**VI. 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 Systems Security Officer  
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  
Telephone: 202-401-5410  
Fax: 202-401-5553  
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:

**VII. APPROVALS**

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

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

<b>Linda Boyer</b> FPLS Information Systems Security Officer	<b>Date</b>
<b>Vicky Turetsky</b> Commissioner	<b>Date</b>

**State Agency Program Official**

<b>Name of State Agency Authorized Official</b> Title of State Agency Authorized Official	<b>Date</b>
<b>Name of State Agency Authorized Official (if two signatures are required)</b> Title of State Agency Authorized Official	<b>Date</b>

## APPENDIX A

### Cost-Benefit Analysis Supplemental Nutrition Assistance Program - National Directory of New Hires Computer Matching Program

Twenty-nine state SNAP agencies implemented the SNAP-NDNH computer matching program in federal fiscal year 2015 to compare information pertaining to applicants for or recipients of SNAP benefits to employment and wage information maintained in the NDNH. Twenty-one state SNAP agencies matched to the NDNH at least one time and provided performance outcomes. After verification of previously unknown earnings, state SNAP agencies collectively reported 95,853 cases that were either closed or benefits were reduced. State SNAP agencies also reported that they avoided approximately \$21 million in improper payments to SNAP 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 SNAP-NDNH computer matching program.

#### Individual State Agency Cost-Benefit Analysis

**Colorado** – Colorado paid \$4,160 to match approximately 326,806 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state matched two times and reported 885 cases closed due to earnings, and 146 cases with benefits reduced. Colorado reported \$326,806 in unduplicated first-month avoided SNAP costs.

**Indiana** – Indiana paid \$9,774 to match approximately 421,033 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state matched nine times and reported 4 cases closed due to earnings, and 41 cases with benefits reduced. Indiana reported \$3,182 in unduplicated first-month avoided SNAP costs.

**Iowa** – Iowa paid \$5,534 to match approximately 274,687 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state matched nine times and reported 3,126 cases closed due to earnings, and 18,530 cases with benefits reduced. Iowa reported \$3,887,990 in unduplicated first-month avoided SNAP costs.

**Kansas** – Kansas paid \$4,459 to match approximately 32,072 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched nine times and reported 21 cases closed due to earnings, and 29 cases with benefits reduced. Kansas reported \$10,618 in unduplicated first-month avoided SNAP costs.

**Maine** – Maine paid \$2,043 to match approximately 198,843 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched six times and reported 537 cases closed due to earnings. Maine reported \$116,562 in unduplicated first-month avoided SNAP costs.

**Maryland** – Maryland paid \$24,715 to match approximately 366,389 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched 12 times and reported 11,057 cases closed due to earnings, and 9,482 cases with benefits reduced. Maryland reported \$2,554,470 in unduplicated first-month avoided SNAP costs.

**Michigan** – Michigan paid \$16,852 to match approximately 183,688 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched nine times and reported 217 cases closed due to earnings, and 22 cases with benefits reduced. Michigan reported \$71,141 in unduplicated first-month avoided SNAP costs.

**Mississippi** – Mississippi paid \$20,492 to match approximately 313,705 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched 10 times and reported 536 cases closed due to earnings, and 7,071 cases with benefits reduced. Mississippi reported \$1,903,946 in unduplicated first-month avoided SNAP costs.

**Missouri** – Missouri paid \$9,543 to match approximately 57,443 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched eight times and reported 92 cases closed due to earnings, and 297 cases with benefits reduced. Missouri reported \$76,552 in unduplicated first-month avoided SNAP costs.

**Montana** - Montana paid \$3,017 to match approximately 21,360 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched 10 times and reported 0 cases closed due to earnings, and 10 cases with benefits reduced. Montana reported \$2,386 in unduplicated first-month avoided SNAP costs.

**New Hampshire** – New Hampshire paid \$2,405 to match approximately 5,762 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched 10 times and reported 0 cases closed due to earnings, and 10 cases with benefits reduced. New Hampshire reported \$2,386 in unduplicated first-month avoided SNAP costs.

**New York** – New York paid \$15,720 to match approximately 345,715 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched five times and reported 16 cases closed due to earnings, and 13 cases with benefits reduced. New York reported \$2,102 in unduplicated first-month avoided SNAP costs.

**North Dakota** – North Dakota paid \$2,388 to match approximately 4,848 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched nine times and reported 185 cases closed due to earnings, and nine cases with benefits reduced. North Dakota reported \$740 in unduplicated first-month avoided SNAP costs.

**Ohio** – Ohio paid \$17,488 to match approximately 124,351 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched 10 times and reported 406 cases closed due to earnings, and 1,089 cases with benefits reduced. Ohio reported \$3,562,403 in unduplicated first-month avoided SNAP costs.

**Pennsylvania** - Pennsylvania paid \$17,847 to match approximately 158,022 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched seven times and reported 884 cases closed due to earnings, and 1,527 cases with benefits reduced. Pennsylvania reported \$1,359,734 in unduplicated first-month avoided SNAP costs.

**Tennessee** - Tennessee paid \$13,585 to match approximately 191,447 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched nine times and reported 1,744 cases closed due to earnings, and 2,532 cases with benefits reduced. Tennessee reported \$882,809 in unduplicated first-month avoided SNAP costs.

**Texas** – Texas paid \$30,737 to match approximately 302,939 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched three times and reported 2,879 cases closed due to earnings, and 3,380 cases with benefits reduced. Texas reported \$2,034,733 in unduplicated first-month avoided SNAP costs.

**Utah** - Utah paid \$3,957 to match approximately 84,166 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched 11 times and reported 6,159 cases closed due to earnings, and 16,265 cases with benefits reduced. Utah reported \$2,693,335 in unduplicated first-month avoided SNAP costs.

**Virginia** - Virginia paid \$10,086 to match approximately 52,877 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched eight times and reported 188 cases closed due to earnings, and 50 cases with benefits reduced. Virginia reported \$769,450 in unduplicated first-month avoided SNAP costs.

**Washington** – Washington paid \$7,899 to match approximately 123,682 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched three times and reported 3,694 cases closed due to earnings, and 2,900 cases with benefits reduced. Washington reported \$1,243,430 in unduplicated first-month avoided SNAP costs.

**Wisconsin** – Wisconsin paid \$5,667 to match approximately 59,697 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched four times and reported 22 cases closed due to earnings, and 78 cases with benefits reduced. Wisconsin reported \$17,873 in unduplicated first-month avoided SNAP costs.

**Wyoming** – Wyoming paid \$2,230 to match approximately 7,021 applicants for or recipients of SNAP benefits to information in the NDNH each month during federal fiscal year 2015. The state agency matched 10 times and reported 26 cases closed due to earnings, and 49 cases with benefits reduced. Wyoming reported \$16,993 in unduplicated first-month avoided SNAP costs.

### **Expected Results of Continued Computer Matching**

Based on the current performance outcome reports, the cost to state SNAP agencies to participate in the SNAP-NDNH matching program is outweighed by the benefit of avoiding improper payments. Because the performance outcome report captures first-month avoided costs, the total of avoided future improper payments is likely to be much greater than what is reported. This is because the SNAP recipients, whose employment and earnings were discovered as a result of the SNAP-NDNH match, likely received an incorrect benefit amount prior to the first month that the match identified the recipients' previously unknown employment. State SNAP agencies are likely to continue to close cases or reduce benefit payments as a result of the SNAP-NDNH computer match, and the first-month cost avoidance is also likely to increase as state SNAP agencies fully implement and continue their SNAP-NDNH matching programs.