COMPUTER MATCHING AGREEMENT

BETWEEN

THE SOCIAL SECURITY ADMINISTRATION

AND

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

"Title II-OCSE Quarterly Match Agreement"
SSA Match #1098/HHS Match #1801

I. PURPOSE

This computer matching agreement, hereinafter "agreement," governs a matching program between the Office of Child Support Enforcement (OCSE) and the Social Security Administration (SSA). The agreement covers the quarterly wage and unemployment insurance batch match for Title II Disability Insurance (DI). OCSE will provide SSA unemployment insurance information if SSA is legally required to use it for the purposes set forth in this agreement. This agreement also governs the use, treatment, and safeguarding of the information exchanged. OCSE is the "source agency" and SSA is the "recipient agency," as defined by the Privacy Act. 5 U.S.C. §§552a(a)(9) and (11).

SSA will use the quarterly wage information to establish or verify eligibility, continuing entitlement, or payment amounts, or all of the above, of individuals under the DI program. SSA will use the unemployment insurance information to establish or verify eligibility, continuing entitlement, or payment amounts, or all of the above, of individuals under the DI program if SSA is legally required to use the unemployment insurance information for such purposes.

The Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988 (CMPPA), provides that no record contained in a system of records (SOR) may be disclosed for use in a computer matching program except pursuant to a written agreement containing specified provisions. 5 U.S.C. §552a(o). SSA and OCSE are executing this agreement to comply with the Privacy Act of 1974, as amended, and the regulations and guidance promulgated thereunder. SSA and OCSE have entered into agreements and recertifications for this match since November 5, 2015.

The SSA component responsible for this agreement and its contents is the Office of Privacy and Disclosure. The responsible component for OCSE is the Division of Federal Systems. This agreement is applicable to personnel, facilities, and information systems of SSA and

OCSE involved in the processing and storage of National Directory of New Hires (NDNH) information. Personnel are defined as employees, contractors, or agents of SSA and OCSE.

This agreement includes a security addendum and two appendices.

II. RESPONSIBILITIES OF THE PARTIES

A. OCSE Responsibilities

1. On a quarterly basis, OCSE will compare the SSA finder file against the quarterly wage files in the NDNH for the purpose set forth in this agreement.

2. OCSE will send a response file to SSA containing the results of the comparison.

3. If SSA is legally required to use unemployment insurance information for the purposes set forth in this agreement, OCSE will begin to provide such information to SSA on a quarterly basis similar to the quarterly wage files.

B. SSA Responsibilities

1. On a quarterly basis, SSA will submit a finder file of DI beneficiaries for comparison by OCSE against the quarterly wage files in the NDNH.

2. SSA will use the quarterly wage information to administer the DI program efficiently as set forth in this agreement.

3. SSA will make the quarterly wage information available to claims adjudicators through its Identity Management System (IDMS) and eWork files within the Completed Determination Record-Continuing Disability Determination file (CDR-CDD) SOR.

4. SSA adjudicators will use the quarterly wage information provided to request a verification of earnings from beneficiaries.

5. If SSA is legally required to use unemployment insurance information for the purposes set forth in this agreement, SSA will request such information on a quarterly basis from the NDNH.

6. SSA will use the unemployment insurance information as set forth in 2, 3, and 4 above if SSA is legally required to use the unemployment insurance information for such purposes.

7. SSA will publish the *Federal Register* notice and the letters to Congress for this agreement.

III. LEGAL AUTHORITY

The legal authorities for disclosures under this agreement are:

1. Section 453(j)(4) of the Social Security Act (Act) provides that OCSE shall provide the Commissioner of Social Security with all information in the NDNH. 42 U.S.C. §653(j)(4).

2. Section 224(h)(1) of the Act provides that the head of any federal agency shall provide information within its possession as the Commissioner of Social Security may require for purposes of making a timely determination of the amount of the reduction, if any, required by section 224 in benefits payable under Title II of the Act. 42 U.S.C. §424a(h).

Disclosures under this agreement shall be made in accordance with 5 U.S.C. §552a(b)(3), which allows disclosure under a routine use that has been published in a systems of records notice as required by the Privacy Act, and also in compliance with the matching procedures in 5 U.S.C. §552a(o), (p), and (r), which describe matching agreements, verification by agencies of information, and the opportunity for individuals to contest agency findings, and the obligations on agencies to report proposals to establish or change matching programs to Congress and the Office of Management and Budget (OMB).

IV. THE JUSTIFICATION FOR THE MATCHING PROGRAM AND ITS ANTICIPATED RESULTS

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

A. The Justification for the Matching Program

For the FY 2016 pilot, the systems selected approximately 1,200 CDR cases using quarterly earnings. Of these 1,200 cases, 22 percent (264 cases) resulted in termination of monthly benefit payments. The average monthly benefit payment amount was $1,166. The total adjustment in terminated monthly payment amount was $307,824. We conservatively predict that without this matching operation these incorrect payments would have continued for seven months, costing SSA $2,154,768. Therefore, in FY 2016, we observed a savings of approximately $2,154,768.

From the FY 2016 pilot, the Office of Research, Demonstration, and Employment Support (ORDES) reported a total overpayment of $9.6 million from beneficiaries working within or after their Extended Period of Eligibility. Based on historical Title II data, we expect to recover 85 percent of these overpaid benefits, for a total benefit of approximately $8,160,000.

For FY 2016, the total benefits realized from this matching operation is approximately $10,314,768.

B. Anticipated Results of the Matching Program

The benefit to the United States Treasury of these combined matching operations includes the correction of those cases when there is a decrease in the monthly payment amount, the recovery of detected overpayments, and the Continuing Disability Review work cost avoidance.

For FY 2016, this matching operation resulted in an estimated overall savings of about 10,314,768. The total costs are approximately $343,828. These savings to the United States Treasury make this matching operation cost effective with a benefit-to-cost ratio of 30:1; therefore, this match is cost effective.

V. DESCRIPTION OF THE RECORDS MATCHED

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. SSA and OCSE Systems of Records

SSA and OCSE published a notice of the relevant SORs in the *Federal Register*. SSA's SORs are the Master Beneficiary Record (MBR), 60-0090 last fully published January 11, 2006 at 71 FR 1826, amended on December 10, 2007 at 72 FR 69723, and amended on July 5, 2013 at 78 FR 40542; and the CDR-CDD file, 60-0050 last fully published January 11, 2006 at 71 FR 1813 and amended on December 10, 2007 at 72 FR 69723.

OCSE will match SSA information in the MBR and CDR-CDD against the quarterly wage information maintained in the NDNH. If SSA is legally required to use unemployment insurance information for the purposes set forth in this agreement, OCSE will match SSA information in the MBR and CDR-CDD against the unemployment insurance information maintained in the NDNH. The NDNH contains new hire, quarterly wage, and unemployment insurance information furnished by state and federal agencies and is maintained by OCSE in its SOR "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 SSA constitutes a "routine use," as defined by the Privacy Act. 5 U.S.C. §552a(b)(3). Routine use (9) of the system of records authorizes the disclosure of NDNH information to SSA for this purpose. 80 FR 17906, 17907 (April 2, 2015).

B. Data Elements Used in the Matching Program

1. SSA will provide electronically to OCSE the following data elements in the finder file:

- Individual's Social Security number (SSN)
- Name (first, middle, last)

2. OCSE will provide electronically to SSA the following data elements from the NDNH in the quarterly wage file:

- Quarterly wage record identifier
- For employees:
  (1) Name (first, middle, last)
  (2) SSN
  (3) Verification request code
  (4) Processed date
  (5) Non-verifiable indicator
  (6) Wage amount
  (7) Reporting period

- For employers of individuals in the quarterly wage file of the NDNH:
  (1) Name (first, middle, last)
  (2) Employer identification number
  (3) Address(es)

- Transmitter agency code
- Transmitter state code
- State or agency name

3. OCSE will provide electronically to SSA the following data elements from the NDNH in the unemployment insurance file if SSA is legally required to use such information for the purposes set forth in this agreement:

- Unemployment insurance record identifier
- Processed date
- SSN
- Verification request code
- Name (first, middle, last)
- Address
- Unemployment insurance benefit amount
- Reporting period
- Transmitter agency code
- Transmitter state code
- State or agency name

SSA will not maintain the unemployment insurance information until SSA is legally required to use it for the purposes set forth in this agreement.

C. Number of Records to Be Matched

The SSA finder file will contain approximately 9.8 million records of individuals.

The NDNH contains approximately 1.4 billion new hire, quarterly wage, and unemployment insurance records, which represent the most recent 24 months of information. In accordance with section 453(j)(4) of the Act, NDNH information provided to SSA by OCSE will contain the available data elements from the quarterly wage information, if any, pertaining to the individuals whose records are contained in the SSA finder file. 42 U.S.C. §653(j)(4).

D. Period of the Matching Program

The starting and completion dates of the matching program are consistent with the effective and expiration dates of this agreement. The matching program will continue in effect until it expires unless terminated as stated in this agreement. SSA will conduct batch matches for DI applicants or beneficiaries with the NDNH database no more frequently than quarterly.

VI. NOTICE PROCEDURES

The Privacy Act requires that the agreement specify procedures for providing individualized notice at the time of application, and periodically thereafter as directed by the Data Integrity Board (DIB), to applicants and recipients of financial assistance or payments under federal benefit programs, that the information they provide may be verified through matching programs. 5 U.S.C. §552a(o)(1)(D).

This requirement is best accomplished by notice provided to the individual on the form in the agency's request for information or on a separate form pursuant to the Privacy Act. 5 U.S.C. §552a(e)(3). SSA and OCSE provide the following notices, respectively, to persons whose records are disclosed from the system of records involved in the matching program established under this agreement.

A. Notice to the General Public

SSA will publish a notice describing SSA's matching activities in the *Federal Register* informing the general public of this specific matching program. Both SSA and OCSE published a notice of the relevant systems of records in the *Federal Register*.

B. Notice to Applicants

SSA will notify individuals at the time of application for DI benefits regarding the comparison of their records against those of other agencies to verify their eligibility or payment amounts. SSA's notice consists of appropriate language printed either on its application forms or on a separate handout when necessary.

C. Notice to Beneficiaries

SSA will notify DI beneficiaries at least once during the life of the agreement and of any extension to this agreement that it will use data from other agencies to verify their eligibility or payment amounts. SSA includes notice to DI beneficiaries in mailings pertaining to work continuing disability reviews (Work CDRs-CDD) and with the annual cost-of-living adjustment notice to all recipients.

VII. VERIFICATION AND OPPORTUNITY TO CONTEST

The Privacy Act requires that each matching agreement specify procedures for verifying information produced in the matching program and an opportunity to contest findings. 5 U.S.C. §552a(o)(1)(E) and (p).

SSA recognizes that the occurrence of a comparison between its files and the NDNH is not conclusive evidence of the address, employer, or wages of an identified individual, but is an indication that warrants further verification.

A. Verification of Information Produced in the Matching Program

SSA verifies the name/SSN combinations in its systems of records. SSA will compare the identity information in its records for the matched individual with the NDNH information and then determine whether the information in the NDNH is consistent with the information in SSA's files. If the information is not consistent, SSA will contact the individual to confirm the information provided by the NDNH.

If the individual is unable to confirm the information, SSA will contact the employer(s) shown by the NDNH quarterly wage file to confirm the information shown by the comparison results. SSA will independently verify the NDNH information, investigate, and confirm information that is used as a basis for an adverse action against an individual, as described in 5 U.S.C. §552a(p)(1) and (2). If SSA is legally required to use unemployment insurance information for the purposes set forth in this agreement, SSA will verify such information similar to SSA's process for verifying quarterly wage information.

B. Opportunity to Contest Findings

SSA will not take action to reduce, suspend, or terminate disability benefits based on information obtained from this matching program until:

1. SSA provides notice to the affected individual that informs the individual of the results of SSA's verification of the information and his or her opportunity to contest the findings.

2. SSA gives the affected individual, under applicable SSA regulations and procedures, 10 days to respond to the notice before SSA takes any adverse action as a result of the comparison information. 20 C.F.R. §404.1595(c).

3. In the event that the individual does not respond to the notice in the required time, SSA concludes that the comparison results provided by OCSE are correct and makes the necessary adjustment to the individual's DI payment.

VIII. ACCURACY ASSESSMENT

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).

The information contained in the NDNH is reported to the source agency by state and federal agencies and instrumentalities. OCSE verifies the accuracy of name and SSN combinations maintained by OCSE against SSA's NUMIDENT file, in accordance with section 453(j)(1)(A) and (B) of the Act. 42 U.S.C. §653(j)(1)(A) and (B). A record reported to the NDNH is considered "verified" if the name and SSN combination have a corresponding name and SSN within SSA's NUMIDENT.

All employee names and SSN combinations contained in the new hire and the unemployment insurance files against which finder files are compared have been verified against SSA NUMIDENT. For quarterly wage, only 77 percent 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.

Based on internal consistency checks and SSN/name verification process before the creation of a payment record, SSA estimates that at least 99 percent of the name and SSN information on the MBR is accurate.

IX. LIMITATIONS ON ACCESS AND USE

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).

A. Limitations on the Use of Information by OCSE

OCSE will adhere to the following limitations on the use of the information contained in the finder files disclosed to OCSE by SSA under the provisions of this agreement:

1. OCSE may not duplicate or disseminate (within or outside OCSE) SSA finder files and the information contained within SSA's files without the written approval of SSA, except as necessary for backup to ongoing operations of the matching program. SSA will not grant such authority unless the disclosure is required by law or is essential to the matching program. Once the matching activity authorized under this agreement is completed, the SSA finder files remain the property of SSA and must be handled as provided in sections X and XI.

2. OCSE may only use or access SSA finder files and information provided by SSA for the purposes specified in this agreement.

3. OCSE may not use SSA finder files to extract information concerning the individuals named within the files for any purpose not specified in the agreement.

B. Limitations on the Use, Duplication, and Redisclosure of Information by SSA

SSA will adhere to the following limitations on the use of information provided by OCSE:

1. SSA may only use NDNH information for the purposes specified in this agreement.

2. SSA may not use NDNH information to extract information concerning the named individuals for any purpose not specified in this agreement.

3. SSA may not duplicate or disseminate NDNH information (within or outside SSA) without the written permission of OCSE, except as necessary for backup to ongoing operations of the matching program and for the purpose of disaster recovery. Permitted paper folder and electronic NDNH duplication or dissemination must be in accord with sections X and XI.C. OCSE will not grant such authority unless the disclosure is required by law or is essential to the matching program.

4. Once matching activity under this agreement is completed, information provided by OCSE remains the property of OCSE and must be handled as provided in sections X and XI.

C. Penalties

Subsection 453(l)(1) of the Act 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, adjusted for inflation, 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). The penalty is subject to inflation adjustment as authorized by the Federal Penalty Inflation Adjustment Improvement Act of 2015 (Section 701 of Pub. L. No. 114-74). *See* 45 CFR §303.21(f) and 42 CFR §102.3.

X. PROCEDURES FOR RETENTION AND TIMELY DESTRUCTION 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 in such matching program. 5 U.S.C. §552a(o)(1)(F).

This section specifies the retention periods for the records contained in the SSA finder file and the NDNH records provided to SSA. After the retention periods, SSA and OCSE shall destroy the records in accordance with the security addendum herein, including the erasure of all electronic records.

OCSE may retain the SSA records contained in the finder file provided by SSA only for the period of time required for the processing related to the matching program, but no later than 60 days after the transmission of the file to OCSE.

SSA agrees to the following procedures for the retention and destruction of identifiable records:

1. SSA will retain the response files received from OCSE only for the period of time required for any processing related to the matching program and will then destroy the response file, unless SSA is required to retain the information in order to meet evidentiary requirements. In case of such retention for evidentiary purposes, SSA will retire the retained data in accordance with the applicable National Archives and Records Administration (NARA) Records Schedule for the MBR and the CDR-CDD system of records. 44 U.S.C. §3303a

2. SSA field office (FO) personnel will dispose of the case file printouts of the comparison results of specific individuals in accordance with the appropriate NARA Records Schedule for the MBR and the CDR-CDD system of records. 44 U.S.C. §3303a

Neither SSA nor OCSE will create a separate file or SOR concerning individuals in the matching program, other than SSA records needed for integrity and audit purposes. Both SSA and OCSE will keep an accurate accounting of disclosures from an individual's records as required by subsection (c) of the Privacy Act.

XI. PROCEDURES FOR SECURITY

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).

SSA and OCSE will comply with the requirements of the Federal Information Security Management Act (FISMA), 44 U.S.C. Chapter 35, Subchapter II, as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); related Office of Management and Budget (OMB) circulars and memoranda, such as Circular A-130, Managing Federal Information as a Strategic Resource (July 28, 2016); National Institute of Standards and Technology (NIST) directives; and the Federal Acquisition Regulations, including any applicable amendments published after the effective date of this agreement. These laws, directives, and regulations include requirements for safeguarding federal information systems and personally identifiable information (PII) used in Federal agency business processes, as well as related reporting requirements. Both agencies recognize, and will implement, the laws, regulations, NIST standards, and OMB directives including those published subsequent to the effective date of this agreement.

FISMA requirements apply to all federal contractors, organizations, or entities that possess or use Federal information, or that operate, use, or have access to federal information systems on behalf of an agency. Both agencies are responsible for oversight and compliance of their contractors and agents.

The security addendum to this agreement specifies these security procedures, and shall be taken and considered as part of this agreement as if the provisions contained in the addendum were fully set out here.

A. Incident Reporting

If either SSA or OCSE experiences an incident involving the loss or breach of PII provided by SSA or OCSE under the terms of this agreement, they will follow the incident reporting guidelines issued by OMB. In the event of a reportable incident under OMB guidance involving PII, the agency experiencing the incident is responsible for following its established procedures, including notification to the proper organizations (e.g., United States Computer Emergency Readiness Team, the agency's privacy office). In addition, the agency experiencing the incident (e.g., electronic or paper) will notify the other agency's Systems Security Contact named in this agreement. If OCSE is unable to speak with the SSA Systems Security Contact within one hour or if for some other reason notifying the SSA Systems Security Contact is not practicable (e.g., it is outside of the normal business hours), OCSE will call SSA's National Network Service Center toll-free at 1-877-697-4889. If SSA is unable to speak with OCSE's Systems Security Contact within one hour, SSA will contact OCSE's Director of Operations at NCC, Baltimore, Maryland 202-596-0494.

B. Breach Notification

SSA and OCSE will follow PII breach notification policies and related procedures issued by OMB. If the agency that experienced the breach determines that the risk of harm requires notification to affected individuals or other remedies, that agency will carry out these remedies without cost to the other agency.

SSA and OCSE will follow PII breach notification policies specified in OMB Memorandum M-17-12 *Preparing for and Responding to a Breach of Personally Identifiable Information* and the incident requirements present in the security addendum. If the agency responsible for the breach determines that the risk of harm requires notification to affected individuals or other remedies, the agency responsible for the breach will carry out these remedies and will bear the costs of breach remediation.

C. Administrative Safeguards

SSA and OCSE will restrict access to the data matched and to any data created by the match to authorized employees and officials who need it to perform their official duties in connection with the uses of the data authorized in this agreement. Further, SSA and OCSE will advise all personnel who have access to the data matched and to any data created by the match of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable federal laws.

D. Physical Safeguards

SSA and OCSE will store the data matched and any data created by the match in an area that is physically and technologically secure from access by unauthorized persons at all times. Only authorized personnel will transport the data matched and any data created by the match. SSA and OCSE will establish appropriate safeguards for such data, as determined by a risk-based assessment of the circumstances involved.

E. Technical Safeguards

SSA and OCSE will process the data matched and any data created by the match under the immediate supervision and control of authorized personnel in a manner that will protect the confidentiality of the data, so that unauthorized persons cannot retrieve any data by computer, remote terminal, or other means. Systems personnel must enter personal identification numbers when accessing data on the agencies' systems. SSA and OCSE will strictly limit authorization to those electronic data areas necessary for the authorized analyst to perform his or her official duties.

F. Application of Policy and Procedures

SSA and OCSE will adopt policies and procedures to ensure that each agency uses the information contained in their respective records or obtained from each other solely as

provided in this agreement. SSA and OCSE will comply with these guidelines and any subsequent revisions.

G. Onsite Inspection

SSA and OCSE have the right to monitor the other party's compliance with FISMA and OMB requirements. Both parties have the right to make onsite inspections for auditing compliance, if necessary, for the duration or any extension of this agreement. If either party elects to complete an onsite inspection, the auditing agency will provide the other advance written notice of any onsite inspection and the parties will set a mutually agreeable date for such inspection.

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 the matching program in the *Federal Register*. 5 U.S.C. §§552a(o)(2)(A)(i) and (ii). Notice of the matching program must be transmitted to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform and OMB at least 30 days before the submission of the notice to the *Federal Register* for publication. *See* 5 U.S.C. §§552a(e)(12) and (r), and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

An agreement is not effective until agencies comply with all notice 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. SSA and OCSE intend that the effective date of this agreement will be June 17, 2018, the day after the expiration date of the amendment and renewal of the matching agreement, U.S. Department of Health and Human Services DIB, No. [TBD].

This agreement shall be effective after the compliance with, or subject to, the following requirements:

- When this agreement is approved and signed by the Chairperson of the HHS DIB, provided that all documents making up the matching program report to OMB and Congress (i.e., the agreement, narrative statement, matching notice, transmittal letters, and any required supplementary documents) have been prepared in full compliance with the Privacy Act and OMB policies (in particular, OMB Circular A-108, Sections 8 and 9 and Appendix V), and SSA then signs the transmittal letters and submits copies of the matching program report to Congress (two hard copies by mail or courier) and OMB (via ROCIS) for their advance review.

- The advance review period for OMB and Congress will begin on the date of submission to OMB in ROCIS and will end 30 days after that date if they make no comments and OMB does not extend the advance review period.
- Upon completion of the advance review period, SSA will forward the public notice of the proposed matching program for publication in the *Federal Register* as required by subsection (e)(12) of the Privacy Act. The matching notice will be effective 30 days after publication if no public comments are received that necessitate changes to the notice.
- SSA will post a copy of the published notice and this agreement to the Internet and will provide a copy of the notice to the other parties to this agreement.

B. Duration of the Agreement

The Privacy Act requires that an agreement shall remain in effect only for such period, not to exceed 18 months, as the DIB 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 a period of 18 months, subject to renewal by the DIB of both agencies for a period of up to 1 year. The DIB of both agencies may, within 3 months prior to the expiration of this agreement, renew this agreement for a period not to exceed 12 months. The renewal may occur if SSA and OCSE can certify in writing to their DIBs that: 1) the matching program will be conducted without change, and 2) SSA and OCSE have conducted the matching program in compliance with the original agreement.

Both SSA and OCSE will sign a form SSA-429 *Agreement Covering Reimbursable Services* and an OCSE reimbursement agreement, prior to the initiation of any services of this agreement and for each fiscal year in which this agreement is in effect.

C. Modification of the Agreement

The parties may modify this agreement at any time by a written modification, agreed to by both parties and approved by the DIB of each agency.

D. Termination of the Agreement

Prior to the agreement's end in accord with section XII.B, the agreement may be terminated in three ways. First, it may be terminated immediately with the consent of both agencies. Second, either agency may unilaterally terminate it by written notice to the other agency. Unilateral termination is effective 90 days after the date of the notice or on a later date, as specified in the notice. Third, either agency may immediately and unilaterally terminate the agreement and any further disclosures if it determines that:

- SSA does not meet its requirement to reimburse OCSE under section 453(k) of the Act as agreed upon in section XV of this agreement and the fiscal agreements of both SSA and OCSE;

- OCSE 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 pursuant to 5 U.S.C. §552a(q)(1);

- Any authorized entity to which NDNH information is redisclosed in accordance with section IX is not complying with any of the terms and provisions in this agreement; or

- The privacy or security of NDNH information is at risk.

Each agency will submit to its DIB a copy of any notification of termination.

XIII. PERIODIC REPORTING OF RESULTS OF THE MATCHING PROGRAM

OMB requires OCSE to periodically report measures of the performance of the Federal Parent Locator Service (FPLS), including the NDNH, through various federal management devices, such as the 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 FPLS supports OCSE's strategic mission, goals, and objectives and cross-agency collaboration. OCSE also requests such performance reporting to ensure matching partners use NDNH information for the authorized purpose.

To assist OCSE in its compliance with federal reporting requirements, and to provide assurance that SSA uses NDNH information for the authorized purpose, SSA must provide to OCSE a written description of the performance outputs and outcomes attributable to its use of NDNH information for the purposes set forth in this agreement.

SSA must provide such reports, in a format determined by SSA and approved by OCSE, to OCSE on an annual basis, no later than two months after the end of each fiscal year of the matching program.

The performance reports may also assist SSA 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).

XIV. 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). SSA and OCSE agree that the Comptroller General may have access to such records for the authorized purpose of monitoring or verifying compliance with this agreement.

XV. REIMBURSEMENT

Pursuant to section 453(k)(3) of the Act, a state or federal agency that receives information from OCSE shall reimburse OCSE for costs incurred in furnishing the information, at rates which OCSE determines to be reasonable. 42 U.S.C. §653(k)(3). SSA will reimburse OCSE for use of NDNH information on an annual fiscal year basis. SSA will reimburse OCSE via a reimbursable agreement (RA) prepared by OCSE, and the Interagency Agreement Data Sheet (Form SSA-429) prepared by SSA and signed by both OCSE and SSA. The Interagency Agreement (IAA) package will include an Form SSA-429, identifying the provisions of the agreement. An RA and Form SSA-429 will be entered into each fiscal year and will address costs and reimbursement terms. The Office of Data Exchange and Policy Publications at SSA is responsible for processing the RA and Form SSA-429. SSA's ability to obligate funds under the RA for each fiscal year is subject to the availability of funds

OCSE will collect funds from SSA through the Intra-Governmental Payment and Collection (IPAC) system. OCSE will bill SSA twice during the fiscal year, in accordance with the amounts and terms outlined in the RA and Form SSA-429. SSA will remit payments no later than 15 days following the receipt of each bill. Additionally, at least quarterly, the parties will reconcile balances related to revenue and expenses for work performed under the agreement. Should SSA receive additional data and/or be legally required to use unemployment information for the purposes set forth in this agreement, during any reimbursement period under this agreement, the reimbursement documents executed for that period will be amended to reflect any additional costs determined by the receipt of additional data during the quarter, to cover OCSE's cost for providing additional information to SSA.

XVI. DISPUTE RESOLUTION

Disputes related to this agreement shall be resolved in accordance with instructions provided in the Treasury Financial Manual (TFM), *Intragovernmental Transaction Guide,* or superseding directive, available on the TFM website at http://tfm.fiscal.treasury.gov.

XVII. PERSONS TO CONTACT FOR FURTHER INFORMATION

A. SSA Contacts:

Program Policy Issues

Kristine Erwin-Tribbitt, Office Director
Office of Program Evaluations
Office of Research, Demonstrations, and Employments Support
Social Security Administration
4302 Annex Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: 410-965-3353
Email: Kristine.Erwin-Tribbitt@ssa.gov

La'Tonya A. Anderson, Social Insurance Specialist
Office of Supplemental Security Income and Program Integrity Policy
Office of Income Security Programs
Social Security Administration
2-R-19-E Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: 410-966-3882
Fax: 410-966-0980
Email: Latonya.Anderson@ssa.gov

Computer Systems Issues

Alan Elkin, Branch Chief
Disability Control Branch
Division of Title II Control & Queries
Office of Systems
4-A-6 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: 410-965-8050
Fax: 410-966-5272
Email: Alan.Elkin@ssa.gov

Matching Agreement Issues

Sonia Robinson, Government Information Specialist
Office of Privacy and Disclosure
Office of the General Counsel
617 Altmeyer Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: 410-966-4115
Fax: 410-966-4304
Email: Sonia.V.Robinson@ssa.gov

Data Exchange Issues

Stephanie Brock, Data Exchange Liaison
Office of Data Exchange and Policy Publications
Office of Retirement and Disability Policy
4-B-7-C Annex Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: 410-965-7827
Email: Stephanie.Brock@ssa.gov

Systems Security Issues

Guy Fortson, Acting Director
Office of Information Security
Division of Compliance and Oversight
Suite 3105 Annex
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 597-1103
Fax: (410) 597-0845
Email: Guy.Fortson@ssa.gov

B. OCSE Contacts:

Linda Boyer, Director
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
Mary E. Switzer Building
330 C Street SW, 5th Floor
Washington, DC 20201
Phone: 202-401-5410
Fax: 202-401-5558
Email: Linda.Boyer@acf.hhs.gov

Maureen Henriksen, OCSE Liaison with SSA for Data Exchange
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 20101
Phone: 202-205-3848
Fax: 202-401-5558
Email: Maureen.Henriksen@acf.hhs.gov

XVIII. INTEGRATION CLAUSE

This agreement, the security addendum, appendices A-D, the accompanying Form SSA-429, the OCSE RA, and the IAA identifying the provisions of the agreement constitute the entire agreement of the parties with respect to its subject matter and supersede all other data exchange agreements between the parties for the purposes described herein. The Form SSA-429, the OCSE RA, and the IAA are prepared and authorized at the start of each fiscal year throughout the life of this agreement. The parties have made no representations, warranties, or promises outside of this agreement. This agreement takes precedence over any other documents potentially in conflict with it, however; it does not supersede federal law or HHS and OMB directives.

XIX. SIGNATURES

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

U.S. Department of Health and Human Services Officials

Scott M. Lekan Commissioner Office of Child Support Enforcement	**Date**
John A. Bardis Chairperson HHS Data Integrity Board	**Date**

SOCIAL SECURITY ADMINISTRATION (SSA)

Monica Chyn Acting Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	**Date**
Mary Ann Zimmerman Acting Chair SSA Data Integrity Board Social Security Administration	**Date**

SECURITY ADDENDUM

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

and

THE SOCIAL SECURITY ADMINISTRATION

Title II-OCSE Quarterly Match Agreement
SSA Match #1098/HHS Match #1801

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 Social Security Administration (SSA) 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 SSA agree to comply with the provisions of the Social Security Act, the Privacy Act of 1974, the Federal Information Security Modernization Act of 2014 (FISMA), Office of Management and Budget (OMB) directives, the National Institute of Standards and Technology (NIST) series of Special Publications (SP), and the underlying agreement to this security addendum. Further, each agency has implemented the minimum security controls required for a system categorized as "moderate" in accordance with the Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. OCSE and SSA agree to use the information (such as input and output files) received from each agency for authorized purposes in accordance with the terms of the agreement.

As federal requirements change or new requirements are established, OCSE and SSA shall comply with such requirements.

II. APPLICABILITY OF THIS SECURITY ADDENDUM

This security addendum is applicable to the agency, personnel, facilities, documentation, information, electronic and physical records, other machine-readable information, and the information systems of OCSE and SSA, and entities specified in the agreement which are hereinafter "OCSE" and "SSA."

III. SECURITY AND PRIVACY SAFEGUARDING REQUIREMENTS

SSA shall comply with the *Office of Child Support Enforcement Division of Federal Systems Security Requirements for Federal Agencies Receiving Federal Parent Locator Service Data*.

SSA received this document on December 7, 2017. The safeguarding requirements in this security addendum are drawn from this document and are also based on the federal laws and requirements governing the protection of information referenced in section I of this security addendum.

This section provides the safeguarding requirements with which OCSE and SSA shall comply and continuously monitor. SSA shall also comply with three additional requirements: Breach Reporting and Notification Responsibility, Security Authorization, and Audit Requirements.

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

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

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

   Policy/Requirements Traceability: 5 U.S.C. §552a(b)(1)

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

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

   Policy/Requirements Traceability: 5 U.S.C. §552a; NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* PL-4(1), PS-6, PS-8

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

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

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

4. SSA 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 threats, and the possible sanctions for misuse. All personnel shall receive security and privacy awareness training before accessing NDNH information and at least annually thereafter. The training shall cover the matching provisions of the federal Privacy Act, the Computer Matching and Privacy Protection Act, and other federal laws governing use and misuse of protected 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 threats, and the possible sanctions for misuse. All personnel receive security and privacy awareness training before accessing agency input files and at least annually thereafter. The training covers the other federal laws governing use and misuse of protected information.

   Policy/Requirements Traceability: 5 U.S.C. §552a; 44 U.S.C. §3551 et seq; OMB Circular A-130, *Managing Information as a Strategic Resource*; OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information;* NIST SP 800-53 Rev 4, AT-2(2), AT-3

5. SSA 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 agreements, rules of behavior, or equivalent documents shall outline the authorized purposes for which the SSA may use NDNH information, the privacy and security safeguards contained in this agreement and security addendum, and the civil and criminal penalties for unauthorized use. SSA may use "wet" and/or electronic signatures to acknowledge non-disclosure agreements, rules of behavior, or equivalent documents.

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

   Policy/Requirements Traceability: OMB Circular A-130 - Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*; OMB M-17-12; NIST SP 800-53 Rev 4, PS-6

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

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

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

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

   OCSE has appropriate procedures in place to report security or privacy incidents, or suspected incidents involving the agency input files. Immediately upon discovery but in no case later than one hour after discovery of the incident, OCSE will report confirmed and suspected incidents to the SSA security contact designated in this security addendum. The requirement for OCSE to report confirmed or suspected incidents to SSA 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 I; OMB M-17-12; NIST SP 800-53 Rev 4, IR-6

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

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

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

9. SSA 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. SSA and non-SSA 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 SSA resources, SSA shall scan the SSA and non-SSA furnished equipment to ensure compliance with SSA standards. All remote connections shall be through Network Access Control, and all data in transit between the remote location and SSA shall be encrypted using FIPS 140-2 encryption standards. Personally owned devices shall not be authorized.

See numbers 8 and 19 of this section for additional information.

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

Policy/Requirements Traceability: OMB-M-17-12; NIST SP 800-53 Rev 4, AC-17, AC-20

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

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

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

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

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

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

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

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

Policy/Requirements Traceability: NIST SP 800-53 Rev 4, PL-2(3), NIST SP 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*

13. SSA shall maintain a plan of action and milestones (and when applicable, a 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. SSA shall update the plan of action and milestones (and when applicable, the corrective action plan) as necessary based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

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

    Policy/Requirements Traceability: NIST SP 800-53 Rev 4, CA-5, NIST SP 800-18 Rev 1

14. SSA shall maintain a baseline configuration of the system housing NDNH information. The baseline configuration shall include information on system components (for example, standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture.

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

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

15. SSA 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 SSA pursuant to numbers 6 and 27 of this section. SSA shall prevent personnel from browsing by using technical controls or other compensating controls.

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

Policy/Requirements Traceability: 5 U.S.C. §552a; NIST SP 800-53 Rev 4, AC-2, AC-3

16. SSA shall transmit and store all NDNH information provided pursuant to this agreement in a manner that safeguards the information and prohibits unauthorized access. All electronic SSA transmissions of information to SSA and entities specified in the agreement shall be encrypted utilizing a FIPS 140-2 compliant product.

    SSA and OCSE exchange data via a mutually approved and secured data transfer method that utilizes a FIPS 140-2 compliant product.

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

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

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

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

18. SSA 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 residing in commercial or public facilities (for example, hotels, convention centers, airports) from accessing, transmitting, or storing the agency input files.

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

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

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

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

20. SSA 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 and capture the date and time of system events and type 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 and capture the date and time of system events and type 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. SSA shall log each computer-readable data extract (secondary store or files with duplicate NDNH information) from any database holding NDNH information and verify that each extract has been erased within 90 days after completing required use. If SSA requires the extract for longer than 90 days to accomplish a purpose authorized pursuant to this agreement, SSA shall request permission, in writing, to keep the extract for a defined period of time, subject to OCSE written approval. SSA shall comply with the retention and disposition requirements in the agreement.

    OCSE does not extract information from the agency input files.

    Policy/Requirements Traceability: OMB M-17-12

22. SSA 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 19 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-17-12

23. SSA 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: 5 U.S.C. §552a

24. SSA shall implement a Network Access Control (also known as Network Admission Control (NAC)) solution in conjunction with a Virtual Private Network (VPN) option to enforce security policy compliance on all SSA and non-SSA remote devices that attempt to gain access to, or use, NDNH information. SSA 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 SSA enterprise environment. SSA shall disable functionality that allows automatic code execution. The solution shall enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing SSA network and resources while maintaining an audit record on users' access and presence on the SSA network. See numbers 8 and 19 of this section for additional information.

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

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

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

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

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

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

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

    Policy/Requirements Traceability: NIST SP 800-53 Rev 4, PE-2, PE-3

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

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

    Policy/Requirements Traceability: NIST SP 800-53 Rev 4, AC-2, PE-2

28. SSA shall label printed reports containing NDNH information to denote the level of sensitivity of the information and limitations on distribution. SSA shall maintain printed reports in a locked container when not in use and shall not transport NDNH information off SSA and permitted entities premises. When no longer needed, in accordance with the retention and disposition requirements in the agreement SSA shall destroy these printed reports by burning or shredding.

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

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

29. SSA 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/exit points) to prevent unauthorized access to computer and support areas.

    Policy/Requirements Traceability: NIST SP 800-53 Rev 4, PE-3

IV. CLOUD SOLUTION (OPTIONAL)

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

security requirements as defined below still must be met regardless of the type of cloud implementation chosen.

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

2. Use of a cloud solution must be approved in advance by OCSE before connectivity to NDNH information can be established.

3. SSA and the cloud service provider must follow the data retention policies agreed upon by SSA and OCSE to ensure that all required statutory requirements are met.

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

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

V. BREACH REPORTING AND NOTIFICATION RESPONSIBILITY

Upon disclosure of NDNH information from OCSE to SSA, SSA is the responsible party in the event of a confirmed or suspected breach of the information, including responsibility for any costs associated with breach mitigation and remediation. Immediately upon discovery, but in no case later than one hour after discovery of the incident, SSA shall report confirmed and suspected incidents, in either electronic or physical form, to OCSE as designated in this security addendum. SSA is responsible for all reporting and notification activities, including but not limited to: investigating the incident; communicating with US-CERT; notifying individuals whose information is breached; notifying any third parties, including the media; notifying any other public and private sector agencies involved; responding to inquiries about the breach; responding to Congressional inquiries; resolving all issues surrounding the information breach; performing any follow-up activities; correcting the vulnerability that allowed the breach; and any other activity as required by OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and other federal law and guidance.

Policy/Requirements Traceability: *US-CERT Federal Incident Notification Guidelines* (April 1, 2017); OMB Circular A130 – Appendix I; OMB M-17-12; NIST SP 800-53 Rev 4, IR-6

VI. SECURITY AUTHORIZATION

OCSE requires systems that process, transmit, or store NDNH information to be granted authorization to operate following the guidelines in NIST 800-37 Revision 1.

1. SSA Security Posture

OCSE requires SSA to demonstrate its security posture before receiving NDNH information and periodically thereafter, by providing a copy of the Authorization to Operate (ATO) for the SSA environment that will house NDNH information on SSA premises.

The SSA ATO was signed on October 14, 2016. OCSE considers the evidence that the SSA environment is in compliance with the security requirements in this security addendum. The effective period for an ATO is three years, which means OCSE maintains the right to request an updated ATO signature if the signature date on file expires during this agreement.

SSA is only authorized to process, transmit, and store NDNH information in the SSA environment and premises.

2. SSA Permitted Entity Security Posture

Prior to the redisclosure of NDNH information by SSA to any authorized entity, SSA shall demonstrate, and OCSE shall review and approve, the security posture of the entity's systems and processes.

All information systems and applications that process, transmit, or store NDNH information shall be fully compliant with FISMA, OMB directives, and NIST guidelines.

Prior to receiving NDNH information, entities shall have implemented the minimum security controls required for a system categorized as "moderate" in accordance with FIPS 199.

All systems and applications handling NDNH information shall first be granted the ATO through the authorization process according to NIST SP 800-37 Revision 1. In addition, if applicable, federal agencies that share NDNH information with entities specified in the agreement shall ensure the specified contractors meet the same safeguarding requirements. The authorizing official of the agency that re-discloses NDNH information to the permitted entity may grant them the ATO or security authorization.

The security authorization process shall have been conducted according to the NIST SP 800-37 Revision 1, as appropriate.

Federal agencies shall comply with NIST SP 800-37 Revision 1, including implementing a continuous monitoring program for permitted entities. Agencies shall conduct the authorization process at least every three years or when there are major changes to a system. Agencies must verify privacy protection periodically through audits and reviews of the systems and procedures.

By signing the security addendum, SSA signatories confirm that SSA has reviewed the

entities specified in the agreement, reviewed the security controls in place to safeguard information and information systems, and determined that the risk to federal data is at an acceptable level. The security controls in place at all entities specified in the agreement are commensurate with those of a federal system categorized as "moderate" according to FIPS 199. *See also* OMB M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements,* October 16, 2017.

VII. AUDIT REQUIREMENTS

The Social Security Act, section 453(m)(2) requires that the Secretary of Health and Human Services establish and implement safeguards with respect to the entities established under section 453 designed to restrict access to confidential information to authorized persons, and restrict use of such information to authorized purposes. 42 U.S.C. §653(m)(2). The Office of Management and Budget guidance provides that since information security remains the responsibility of the originating agency, procedures should be agreed to in advance that provide for the monitoring over time of the effectiveness of the security controls of the recipient organization. OMB M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*. *See also* section 453(l)(2) of the Social Security Act. 42 U.S.C. §653(l)(2) and 5 U.S.C. §552a(e)(10).

Policy/Requirements Traceability: OMB M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements,* October 16, 2017; OMB Circular No. A-130, Appendix I

IV. 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, Director
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
Mary E. Switzer Building
330 C Street SW, 5th Floor
Washington, DC 20201
Phone: 202-401-5410
Fax: 202-401-5553
Email: Linda.Boyer@acf.hhs.gov

B. The SSA security contact is:

Guy Fortson, Acting Director
Office of Information Security
Division of Compliance and Oversight
Suite 3105 Annex
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 597-1103
Fax: (410) 597-0845
Email: Guy.Fortson@ssa.

VIII. APPROVALS

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

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

Linda Boyer Director, Division of Federal Systems Office of Child Support Enforcement	**Date**
Scott M. Lekan Commissioner Office of Child Support Enforcement	**Date**

B. Social Security Administration

Guy Fortson Acting Director Division of Compliance and Assessments Office of Information Security Office of Systems	**Date**
Monica Chyn Acting Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	**Date**

APPENDIX A

DEFINITIONS

FOR

THE COMPUTER MATCHING AGREEMENT

BETWEEN

SSA AND OCSE

"Title II-OCSE Quarterly Match Agreement"
SSA Match #1098/HHS Match #1801

The Privacy Act , 5 U.S.C. §552a(a), defines the terms contained in this agreement.

Additional terms defined as follows:

"CDR-CDD" means Completed Determination Record-Continuing Disability Determination File. This SSA system of records (SOR) is SSA's post-entitlement master record for SSDI and SSI beneficiaries receiving a disability-related benefit including Ticket program beneficiaries.

"Disclose" and **"disclosure"** mean the release of information or data by either SSA or OCSE, with or without the consent of the individual or individuals to which the information pertains.

"FIPS" means Federal Information Processing Standards, a numeric code, issued by the National Bureau of Standards, which identifies every State and local child support agency to facilitate interstate processing.

"State" means any of the 50 states, the District of Columbia, and territories.

Appendix B

Business Needs Assessment Chart
for the Agreement between SSA and OCSE
Covering the Title II NDNH Quarterly Batch
SSA Match #1098/HHS Match #1801

SSA Application	Match Method	Function	Elements Provided by SSA to Conduct Match	Elements Provided by OCSE to Conduct Match	SSA User	Elements temporarily displayed if a match is found	OCSE Databases	Authority
Master Beneficiary Record (MBR) and Completed Determination Record-Continuing Disability Determination file (CDR-CDD)	Batch	To establish and verify eligibility or payment amounts, or both under the SSI program	Individual's Social Security number (SSN) and Name	From the Quarterly Wage File: quarterly wage record identifier; for employees: name, SSN, verification request code, processed date, non-verifiable indicator, wage amount, and reporting period; for employers of individuals: name, employer identification number (EIN), and addresses; transmitter agency code, transmitter state code, state or agency name. From the Unemployment Insurance File: unemployment insurance record identifier, processed date, SSN, verification request code, name, address, unemployment insurance benefit amount, reporting period, transmitted agency code, transmitter state code, and state or agency name.	SSA claims personnel responsible for determining eligibility for DI	Quarterly wage record identifier, name, SSN, processed date, address(es), wage amount, quarterly wage reporting period. Employers name, transmitted agency code employer address(es). Unemployment insurance record identifier, processed date, unemployment insurance benefit amount, and reporting period.	National Directory of New Hires (NDNH) - Quarterly Wage File and Unemployment Information File	42 U.S.C. § 653(j)(4)

Cost Benefit Analysis (CBA) for the Computer Matching Agreement (CMA) between The Social Security Administration (SSA) and The Department of Health and Human Services, Administration for Children and Families, Office of Child Support Enforcement (OCSE)

(SSA's Master Beneficiary Record (MBR) and Completed Determination Record – Continuing Disability Determination (CDR-CDD) and OCSE's National Directory of New Hires (NDNH) Quarterly Wage File (Match #1098)

Objective

The purpose of this CBA is to determine the cost-effectiveness of the matching operation between SSA's MBR and CDR-CDD and OCSE's NDNH Quarterly Wage File.

Background

Since September 1998, SSA has performed a quarterly automated data matching operation between the OCSE's NDNH Quarterly Wage file and the Supplemental Security Record (SSR). The purpose of this matching operation, under CMA #1074, is to identify unreported, under-reported or over-reported wage income for Supplemental Security Income recipients and deemors.

In April 2004, SSA and OCSE expanded CMA #1074 to permit authorized SSA employees to use the NDNH online query to develop work activity when processing Title II Disability Insurance (DI) Continuing Disability Reviews (CDRs), Ticket-to-Work initiative cases, and to resolve earnings discrepancies.

Finally, in June 2015, SSA and OCSE signed CMA #1098 to perform a matching operation between SSA's MBR and CDR-CDD and OCSE's NDNH Quarterly Wage File. SSA uses the quarterly wage file from OCSE to establish or verify eligibility, continuing entitlement, payment amounts, or all of the above, of individuals under the DI program.

Methodology

In fiscal year (FY) 2016, the Office of Research, Demonstration, and Employment Support (ORDES) and the Office of Disability Information Systems (ODIS) conducted a pilot for the matching operation under CMA #1098. Due to resource constraints, the matching operation did not run on a quarterly basis, as proposed. ORDES received the data below from ODIS from system runs in July 2016 and August 2016.

- Records sent to OCSE in July 2016 - 52,344,106
- Records sent to OCSE in August 2016 - 52,485,680
- Records returned from OCSE in August 2016 - 6,162,578 (This count may include duplicate SSNs)

The Office of Data Exchange (ODX) examines the ORDES findings of the FY 2016 pilot in this CBA report.

COSTS

The total FY 2016 personnel and computer costs for this matching operation is **$343,828**
Key Element 1: Personnel Costs
For Agencies –

- Source Agency (OCSE) – N/A
- Recipient Agency (SSA)

  Field Office Development

  For FY 2016, the Office of Public Service and Operations Support (OPSOS) reported an average time of 154 minutes to develop work activity for a CDR. Using 154 minutes per case, the total development cost for the 1,200 CDRs developed during the FY 2016 pilot were **$260,018**.

  In addition, the FO incurs costs in incorrect payment development and recovery processing for the 264 cases identified with an overpayment. The FY 2016 cost per case, established by the Division of Cost Analysis in the Office of Financial Policy and Operations is $68.45. Using $68.45 for each overpaid recipient, the total additional development and recovery cost in FY 2016 was **$18,071**.

- Justice Agency – (N/A)

For Clients – N/A
For Third Parties – N/A
For the General Public – N/A
Key Element 2: Agencies' Computer Costs
For Agencies -

- Source Agency (OCSE) – N/A
- Recipient Agencies (SSA)

  For the FY 2016 pilot, ODIS reports an FY 2016 estimated systems (computer) cost of **$58,239**.

- Justice Agencies -N/A

Interagency Agreement Cost

For FY 2016, the total cost of the IAA for this matching operation is **$7,500**.

BENEFITS

Key Element 3: Avoidance of Future Improper Payments

To Agencies –

- Source Agency (OCSE)
- Recipient Agency (SSA)

  The benefits realized from this matching operation include the termination of incorrect monthly benefit payment amounts and the detection and recovery of retroactive overpayments.

For FY 2016, the total benefits realized from this matching operation is approximately **$10,314,768.**

Avoidance of future improper payments

Termination of monthly benefit payment amount

For the FY 2016 pilot, the systems selected approximately 1,200 CDR cases using quarterly earnings. Of these 1,200 cases, 22 percent (264 cases) resulted in termination of monthly benefit payments. The average monthly benefit payment amount was $1,166. The total adjustment in terminated monthly payment amount was $307,824. We conservatively predict that without this matching operation these incorrect payments would have continued for 7 months, costing SSA $2,154,768. Therefore, in FY16, we observed a savings of approximately **$2,154,768**.

- Justice Agencies (N/A)

To Clients – N/A
To the General Public – N/A

Key Element 4: Recovery of Improper Payments and Debts

To Agencies –

- Source Agency (OCSE) – N/A
- Recipient Agency (SSA)

Recovery of improper payments and debts

Retroactive overpayments

From the FY 2016 pilot, ORDES reports a total overpayment of $9.6 million from beneficiaries working within or after their Extended Period of Eligibility. Based on historical Title II data, we expect to recover 85 percent of these overpaid benefits, for a total recovery benefit of approximately **$8,160,000**.

- Justice Agency – N/A

To Clients – N/A
To the General Public – N/A

Conclusion

For FY 2016, this matching operation resulted in an estimated overall savings of about **$10,314,768**. The total costs are approximately **$343,828**. These savings to the United States Treasury make this matching operation cost effective with a benefit-to-cost ratio of **30:1**; therefore, this match is cost effective. Accordingly, we recommend the continuance of this match.

CBA for the Quarterly Batch Matching Operation between the SSR and OCSE's NDNH

Costs

Systems Costs	$58,239
Interagency Agreement (FY 2016)	$7,500
Field Office Alert Development Costs	$260,018
Overpayment Development/Recovery Processing	$18,071
Total Costs	**$343,828**

Benefits

Retroactive Overpayments

Total Overpayment Reported	$9.6 million
Amount Expected to Recover (85%)	$8,160,000

Terminated Monthly Payment Amount

Percent of cases w/Terminated Monthly Payment	22%
Average Monthly Payment Amount	$1,166
Total Monthly Payment Amount	$307,824
Ongoing Monthly Payment (Projected 7 months)	$2,154,768
Total benefits	**$10,314,768**
Benefit to Cost Ratio:	**30:1**

Benefit Computation

Retroactive Overpayments

$9,600,000 x 85% (expected recovery rate)	$8,160,000

Terminated Monthly Payment Amount

Number of term. records (1,200 x 22% = 264)	264
264 x $1,166 (average monthly benefit amt.)	$307,824
$307,824 x 7 (number of months payment cont.)	$2,154,768

Costs Computation

Field Office CDR Work Development/Overpayment Development Costs

Total number of alerts released FY 2012	1200
Salary[1]	$94,897
Development Time per Alert[2]	154 minutes

Work CDR Alert Development Costs

154 minutes x 1.85 overhead[3] (Rounded)	= 285 minutes per Alert
285 minutes x 1200 alerts = (342,000/60)/2080	= 2.74 WY
2.74 WY x $94,897 (Salary) (Rounded)	= $260,018

Overpayment Development and Recovery Costs

Number of Alerts with Overpayments	
264 (Wage alerts with overpayments) x $68.45	= $18,071