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 #2302

I. PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

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 (QW) batch match for Title II Disability Insurance (DI). This agreement also governs the use, treatment, and safeguarding of the QW 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).

A. Purpose of the Matching Agreement

The Privacy Act, as amended by the Computer Matching and Privacy Protection Act of 1988, 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 renewals for this match since November 5, 2015. See Appendix A.

SSA will use the QW information to establish or verify eligibility, continuing entitlement, or payment amounts, or all of the above, of individuals under the DI program.

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 four appendices.

B. Legal Authority

The legal authorities for disclosures under this agreement are the Social Security Act (Act) and the Privacy Act of 1974, as amended. 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). Section 453(j)(4) authorizes OCSE to provide the Commissioner of Social Security with all information in the NDNH. 42 U.S.C. § 653(j)(4). Disclosures under this agreement shall be made in accordance with 5 U.S.C. § 552a(b)(3), under a routine use published in a systems of records notice as required by the Privacy Act, and in compliance with the matching procedures in 5 U.S.C. § 552a(o), (p), and (r), which describes matching agreements, verification by agencies of information, the opportunity for individuals to contest agency findings, and the obligations of agencies to report proposals to establish or change matching programs to Congress and the Office of Management and Budget (OMB).

C. Definitions

See Appendix B.

II. JUSTIFICATION 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. Cost Benefit Analysis

The Privacy Act provides that a Data Integrity Board (DIB) shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective. Unless statutorily excepted or waived by the DIB, a cost benefit analysis must be completed and submitted to the DIB or the DIB cannot approve the matching agreement. See Appendix. D

Comparison of NDNH data with the specified SSA programs results in significant recovery of, or avoidance of, overpayments. For the fiscal year (FY) 2021, the systems selected approximately 118,993 continuing disability review (CDR) cases using quarterly earnings. Of these 118,993 cases, 10,728 cases resulted in a cessation of monthly benefit payments. The average monthly benefit payment amount was $1,214. It is conservatively predicted that without this matching operation these incorrect payments would have continued for eight months, costing SSA $104,190,336. Therefore, in FY 2021, a savings of approximately $104,190,336 was observed.

Details of the Cost Benefit Analysis (CBA) are found in Appendix D.

B. Other Supporting Justifications

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 agencies and Congress efforts to reduce such payments. The OMB issued implementing guidance to federal agencies in Appendix D to Circular A-123, *Requirements for Effective Estimation and Remediation of Improper Payments*, (amended October 20, 2014).

The NDNH is the only nationally centralized directory of new hire, QW, and unemployment insurance information, and, as such, provides an effective, efficient, and comprehensive method of collecting and comparing this information. SSA's use of NDNH QW information supports program accuracy, program administration, and reduces overpayments. There is no other administrative activity that accomplishes the same purpose, provides the same security safeguards, and has the same degree of efficiency.

C. Specific Estimate of Any Savings

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

III. RECORDS DESCRIPTION

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

A. Systems of Records (SORs)

The NDNH contains new hire, QW, and unemployment insurance information furnished by state and federal agencies and is maintained in the SOR "OCSE National Directory of New Hires," System No. 09-80-0381, published in full at 87 Federal Register (Fed. Reg.) 3553 (January 24, 2022). 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 SOR authorizes the disclosure of NDNH records to SSA. 87 Fed. Reg. 3553, 3555 (January 24, 2022).

SSA's relevant SORs are the Master Beneficiary Record (MBR), 60-0090, last fully published on January 11, 2006 at 71 Fed. Reg. 1826, amended on December 10, 2007 at 72 Fed. Reg. 69723, July 5, 2013 at 78 Fed. Reg. 40542, July 3, 2018 at 83 Fed. Reg. 31250-31251, and last amended on November 1, 2018 at 83 Fed. Reg. 54969; the

Completed Determination Record (CDR)-Continuing Disability Determinations (CDD) file, 60-0050, last fully published January 11, 2006 at 71 Fed. Reg. 1813, amended on December 10, 2007 at 72 Fed. Reg. 69723, on November 1, 2018 at 83 Fed. Reg. 54969, and last amended on April 26, 2019 at 84 Fed. Reg. 17907.

The information in these SORs may be updated during the effective period of this agreement as required by the Privacy Act.

OCSE will match SSA information in the MBR and CDR-CDD against the QW information maintained in the NDNH.

B. Number of Records Involved

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

The NDNH contains approximately 1.6 billion new hire, QW, 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 QW information, if any, pertaining to the individuals whose records are contained in the SSA finder file. 42 U.S.C. § 653(j)(4).

Specified Data Elements Used in the Match

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 QW file:**

   - QW 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 QW 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

C. Frequency of Data Exchanges

OCSE Responsibilities

1. On a quarterly basis, OCSE will compare the SSA finder file against the QW 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.

SSA Responsibilities

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

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

3. SSA will make the QW information available to claims adjudicators through its Integrated Disability Management Systems and eWork files within the CDR-CDD SOR.

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

5. SSA will provide advance notice of the matching program to Congress and OMB and, upon completion of OMB's review, will publish the *Federal Register* notice.

D. Projected Start and Completion Dates

The matching program will continue in effect until it expires, unless terminated, renewed, or modified, as stated in this agreement. SSA will conduct batch matches for DI applicants or beneficiaries with the NDNH database no more frequently than quarterly. OCSE may commence comparisons and disclosures under this agreement upon completion of all of the following requirements:

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

IV. NOTICE PROCEDURES

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

The Privacy Act requires that the matching agreement specify procedures for providing individualized notice at the time of application, and notice periodically thereafter, subject to guidance provided by the Director of OMB, 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).

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 will provide the following notices, respectively, to persons whose records are disclosed from the SOR involved in the matching program established under this agreement.

1. 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.

2. 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.

B. Constructive Notice of Matching Program

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

SSA will publish a notice of the matching program in the *Federal Register* at least 30 days before conducting the program and will make the notice and this agreement available on the SSA computer matching agreement internet site; these publications will provide constructive notice of the matching program to affected individuals. SSA will not publish the *Federal Register* notice until SSA has reported the matching program to OMB and Congress for advance review and OMB has completed its review, as required

by 5 U.S.C. § 552a(o)(2)(A) and (r) and OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

V. VERIFICATION PROCEDURES AND OPPORTUNITY TO CONTEST FINDINGS

The Privacy Act 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 Procedures

SSA verifies the name/SSN combinations in its SORs. 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 QW 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).

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 or unless:

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. Under applicable SSA regulations and procedures, the affected individual is given 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(a-c); and

3. The notice clearly states that, unless the individual responds to the notice in the required time, SSA will conclude that the comparison results provided by OCSE are correct and will make the necessary adjustment to the DI benefit.

VI. DISPOSITION OF MATCHED ITEMS

The Privacy Act requires that each matching agreement specify procedures for the retention and timely destruction of identifiable records created by a recipient agency in such matching program 5 U.S.C. § 552a(o)(1)(F).

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

A. SSA Records in the Input File

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

B. NDNH Records in the Output File

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

1. SSA will store and retain the electronic and paper comparison files of the batch match only for the period of time required to support the matching program and will then destroy the records. NDNH information will not be duplicated or disseminated within or outside SSA without the written permission of OCSE, except as necessary within SSA for ongoing operations of the matching program or for the purpose of disaster recovery. OCSE will not grant such authority unless the disclosure is required by law or is essential to the matching program.

2. SSA will store, view, and use the information only for the period of time required for any processing related to the case and will then delete the electronic and/or paper record.

3. SSA will retain the response files identifiable records generated based upon matching NDNH information only for the period required for any processing related to the matching program and will then destroy the response files and records. SSA will destroy all information obtained from OCSE under this agreement in accordance with the applicable Federal Records Retention Schedule. 44 U.S.C. Chapter 33.

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.

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).

SSA and OCSE will comply with the requirements of the Federal Information Security Management Act of 2002, as amended by the Federal Information Security and Modernization Act of 2014 (FISMA), 44 U.S.C. § 3541 et seq., related OMB circulars and memoranda, such as Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016); and National Institute of Science and Technology (NIST) standards. These laws, directives, and standards include requirements for safeguarding federal information systems and personally identifiable information (PII) used in federal agency business processes, as well as related reporting requirements. The laws, OMB directives, and NIST standards relating to the subject of this agreement, including those published subsequent to the effective date of this agreement, must be implemented by both agencies.

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 the oversight, and the compliance, of their contractors and agents.

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

A. Loss Reporting

If either SSA or OCSE experiences an incident involving a 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 (US-CERT) and the agency's privacy office. In addition, the agency experiencing the incident 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 877-697-4889. If SSA is unable to speak with OCSE's Systems Security Contact within one hour, SSA will email the OCSE Incident Mailbox at ocsesecurity@acf.hhs.gov.

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.

C. Administrative Safeguards

SSA and OCSE will restrict access to the data matched and to any data created by the match to only those users (e.g., employees, contractors, etc.) 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 person at all times (e.g., door locks, card keys, biometric identifiers, etc.). 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 for 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. Security Assessment

NIST Special Publication (SP) 800-37 Rev 2 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018), encourages agencies to accept each other's security assessment in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. NIST SP 800-37, as revised, further encourages that this type of reciprocity is best achieved when agencies are transparent and make available sufficient evidence regarding the security state of an information system so that an authorizing official from another organization can use that evidence to make credible, risk-based decisions regarding the operation and use of that system or the information it processes, stores, or transmits. Consistent with that guidance, the parties agree to make available to each other upon request system security evidence for the purpose of making risk-based decisions. Requests for this information may be made by either party at any time throughout the duration or any extension of this agreement.

VIII. RECORDS USAGE, DUPLICATION, AND REDISCLOSURE RESTRICTIONS

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

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

OCSE will adhere to the following limitations on the use of the information contained in SSA's finder files and the information SSA discloses to OCSE under the provisions of this agreement.

1. OCSE will not duplicate or disseminate SSA finder files, the information contained therein, and the information submitted within or outside OCSE without the written approval of SSA, except as necessary within OCSE as backup for 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. The SSA finder files remain the property of SSA. OCSE will handle the files as provided in section VI once the matching activity authorized under this agreement is completed.

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

3. OCSE will not use SSA finder files or information provided by SSA to extract information concerning the individuals therein for any purpose not specified in the agreement.

SSA will adhere to the following limitations on the use of the information OCSE provides to SSA.

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

2. SSA will not use or redisclose the NDNH information to extract information concerning the individuals therein for any purpose not specified in this agreement.

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

4. Information provided by OCSE remains the property of OCSE. SSA will handle the files as provided in section VI once matching activity under this agreement is completed.

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(1)(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 Unites States or any other person who knowingly and willfully violates the requirement. 42 U.S.C. § 653(l)(2). These fines are subject to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015. (Section 701 of Pub. L. No. 114-74). See 45 C.F.R. § 303.21 (f) and 45 C.F.R. Part 102.3.

IX. RECORDS ACCURACY ASSESSMENTS

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

A. NDNH Records

The information 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 Master File of SSN Holders and SSN Applications (Enumeration System), 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 Enumeration System.

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 QW, 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. SSA Records

SSA does not have an accuracy assessment specific to the data elements listed in this agreement. However, SSA conducts periodic statistically valid stewardship (payment accuracy) reviews in which the benefits or payments listed in this agreement are included as items available for review and correction. SSA quality reviewers interview the selected Old Age, Survivors, and Disability Insurance and Supplemental Security Income beneficiaries/recipients and redevelop the non-medical factors of eligibility to determine whether the payment was correct. Based on the available study results (see FY 2020 Title II Payment Accuracy Report, August 2021), there is a reasonable assurance that SSA's accuracy assumptions of a 95 percent confidence level for the monthly benefits or payments listed in this agreement are accurate.

X. COMPTROLLER GENERAL ACCESS

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

XI. REIMBURSEMENT/FUNDING

This agreement does not authorize OCSE to incur obligations through the performance of services described herein. The authority to perform such services requires the execution of the Reimbursement Agreement (RA), and Fiscal Service (FS) Forms 7600A and 7600B. Moreover, OCSE may incur obligations by performing services under this agreement only on a FY basis. An RA and FS Forms 7600A and 7600B are incorporated herein by reference. To the extent, any inconsistency exists between the terms of this agreement and the RA conditions, the terms of this agreement take precedence and control the relationship between SSA and OCSE.

Since OCSE's performance under this agreement spans multiple FYs, SSA will prepare FS Forms 7600A and 7600B at the beginning of each succeeding fiscal year during which OCSE will incur obligations through the performance of the services described herein. Such forms

will be signed by the parties on or before the commencement of the FY. OCSE's ability to provide service in all fiscal years of this agreement is subject to the availability of funds.

Pursuant to section 453(k)(3) of the Act, a state or federal agency that receives information from OCSE must 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 (FY) basis. SSA will reimburse OCSE via a reimbursement agreement prepared by OCSE, SSA prepared FS Forms 7600A and 7600B, and all documents signed by both OCSE and SSA. A reimbursement agreement will be entered into each fiscal year and will address costs and reimbursement terms, which forms are processed by SSA's Office of Data Exchange, Policy and Publications, and International Negotiations. SSA may incur obligations only on a fiscal year basis. SSA's ability to perform work for fiscal years beyond FY 2022 is subject to the availability of funds.

OCSE will collect funds from SSA during FY 2023 and beyond through Treasury's G-invoicing system, which will generate an IPAC sufficient to reimburse OCSE for the costs it has incurred for performing services through the date of billing. OCSE will bill SSA twice during the fiscal year, in accordance with the amounts and terms outlined in the RA and FS Forms 7600A and 7600B. 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.

XII. DURATION OF AGREEMENT

A. Effective Date of the Agreement

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

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

Both SSA and OCSE will sign FS Forms 7600A and 7600B and an OCSE reimbursement agreement prior to the initiation of any services in this agreement and for each fiscal year in which this agreement is in effect. The Privacy Act, as amended, provides that a copy of each matching agreement must be transmitted to the Committee on Homeland Security and Government Affairs of the Senate and the Committee on Oversight and Government

Reform of the House of Representatives 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(o)(2)(A) and (r). OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, requires agencies to report to OMB and Congress any proposal to re-establish a matching program and to continue a program past the expiration of the current matching agreement, at least 60 days prior to the expiration of the existing matching agreement.

Subsection (q) of the Privacy Act 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).

SSA and OCSE intend that the effective date of this agreement will be June 23, 2023, the day after the expiration date of the existing matching agreement, HHS DIB, No. 2007, which was amended and renewed through June 22, 2023.

B. Modification of the Agreement

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

C. Termination of the Agreement

Prior to the agreement's end in accord with this section, 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 XI of this agreement and the fiscal agreements of both SSA and OCSE or 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 VIII 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 PERFORMANCE OUTCOMES

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

To assist OCSE in its compliance with federal reporting requirements, and to provide assurance that SSA uses NDNDH information for the authorized purpose, SSA shall provide OCSE with 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 OCSE, and approved by OMB in accordance with the Paperwork Reduction Act, to OCSE on an annual basis, no later than three months after the end of each fiscal year of the matching program.

The performance reports may also assist in the development of a cost benefit analysis of the matching program required for any subsequent matching agreements in accordance with 5 U.S.C. § 552a(o)(1)(B). See section II.A of this agreement.

XIV. DISPUTE RESOLUTION

Disputes related to this agreement shall be resolved in accordance with instructions provided in the Treasury Financial Manual (TFM), Volume I, Part 2, Chapter 4700, Appendix 5, *Intragovernmental Transaction Guide*.

XV. PERSONS TO CONTACT

A. The U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Enforcement contacts for programs and security are;

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

Maureen Henriksen, Data Access Manager
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
Mary E. Switzer Building
330 C Street, 5th Floor
Washington, DC 20101
Phone: (202) 205-3848
Email: Maureen.Henriksen@acf.hhs.gov

System Security Issues
Charlotte Hancock, NSC-OCSE/DFS Data Center Operations Manager
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
6201 Security Boulevard, NSC-289
Baltimore, MD 21235
Phone: (410) 965-5634
Email: Charlotte.Hancock@acf.hhs.gov

B. Social Security Administration contacts are:

Program Policy Issues

Kristine Erwin-Tribbitt, Senior Advisor
Office of Employment Support
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

Systems Issues

Mary Lindauer, Branch Chief
Disability Review and Work Incentives Branch
DDOAA
3604-RMB Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 966-6581
Email: Mary.D.Lindauer@ssa.gov

Matching Agreement Issues

Sonia Robinson, Government Information Specialist
Office of Privacy and Disclosure
Office of the General Counsel
6401 Security Boulevard, G-401 WHR
Baltimore, MD 21235-6401
Phone: (410) 966-4115
Email: Sonia.V.Robinson@ssa.gov

Data Exchange Issues

Stephanie Brock, Senior Data Exchange Liaison
Office of Data Exchange and International Agreements
Office of Data Exchange, Policy Publication, and International Negotiations
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-4025
Email: Stephanie.Brock@ssa.gov

Fern Parson-Hill, Data Exchange Liaison
Office of Data Exchange, Policy Publications, and International Negotiations
Office of Retirement and Disability Policy
6401 Security Blvd
Baltimore, MD 21235-6401
Phone: (410) 966-3697
Email: Fern.Parson-Hill@ssa.gov

Stephanie Meilinger, Data Exchange Liaison
Office of Data Exchange, Policy Publications, and International Negotiations
Office of Retirement and Disability Policy
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 966-0476
Email: Stephanie.Meilinger@ssa.gov

Systems Security
Jennifer Rutz, Director
Division of Compliance and Oversight
Office of Information Security
Office of Systems
Social Security Administration
Suite 3383, Perimeter East Building
6201 Security Boulevard
Baltimore, MD 21235
Phone: (410) 966-8253
Email: Jennifer.Rutz@ssa.gov

XVI. INTEGRATION CLAUSE

This agreement, the Security Addendum, the appendices, FS Forms 7600A and 7600B, and the OCSE reimbursement agreement prepared and authorized at the start of each fiscal year throughout the life of this 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 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.

XVII. APPROVALS

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

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

Electronic Signature Acknowledgment: The signatories may sign this document electronically by using an approved electronic signature process. By signing this document electronically, the signatory agrees that the signature they provide has the same meaning and legal validity and effect as a handwritten signature.

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

Tanguler S. Gray -S Digitally signed by Tanguler S. Gray -S Date: 2022.11.14 22:22:38 -05'00'	
Tanguler Gray Commissioner Office of Child Support Enforcement	**Date**

B. Social Security Administration (SSA)

Michelle Christ Digitally signed by Michelle Christ Date: 2022.11.16 11:43:13 -05'00'	
Michelle L. Christ Acting Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	**Date**

C. Data Integrity Boards

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

Cheryl R. Campbell -S Digitally signed by Cheryl R. Campbell -S Date: 2023.01.31 14:31:04 -05'00'	
Cheryl Campbell Chairperson	**Date**

Social Security Administration Data Integrity Board

Matthew Ramsey Digitally signed by Matthew Ramsey Date: 2022.12.18 20:50:37 -05'00'	
Matthew D. Ramsey 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 #2302

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) must have in place to ensure the security of the records compared against records in the National Directory of New Hires (NDNH) and the results of the information comparison.

By signing this security addendum, 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 must comply with such requirements.

II. APPLICABILITY OF THIS SECURITY ADDENDUM

This security addendum is applicable to the agency, personnel, facilities, documentation, information, electronic 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

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

This section provides the safeguarding requirements which OCSE and SSA must meet and continuously monitor to ensure compliance. SSA must 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 must restrict access to, and disclosure of, NDNH information to authorized personnel who need NDNH information to perform their official duties in connection with the authorized purposes specified in the agreement.

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

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

2. SSA must 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 5, PL-4(1), PS-6, PS-8

3. SSA must advise all authorized personnel who will access NDNH information of the confidentiality of NDNH information, the safeguards required to protect NDNH information, and the civil and criminal sanctions for non-compliance contained in the applicable 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 5, PL-4(1), PS-6, PS-8

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

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

5. SSA personnel with authorized access to NDNH information must sign non-disclosure agreements, rules of behavior, or equivalent documents before system access, annually, and if changes in assignment occur. The non-disclosure agreement, rules of behavior, or equivalent documents must outline the authorized purposes for which the 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 annually.

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

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

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

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

7. SSA must have appropriate procedures in place to report confirmed and suspected security or privacy incidents (unauthorized use or disclosure involving personally identifiable information), involving NDNH information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, SSA must report confirmed and suspected incidents 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 A-130 – Appendix I; OMB M-17-12; NIST SP 800-53 Rev 5, IR-6

8. SSA must 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 5, AC-20(1)(2)

9. SSA must require that personnel accessing NDNH information remotely (for example, telecommuting) adhere to all the security and privacy safeguarding requirements provided in this security addendum. SSA and non-SSA furnished

equipment must have appropriate software with the latest updates to protect against attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Before electronic connection to SSA resources, SSA must scan the SSA and non-SSA furnished equipment to ensure compliance with SSA standards. All remote connections must be through Network Access Control, and all data in transit between the remote location and SSA must be encrypted using FIPS 140-2 encryption standards. Personally owned devices must 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 5, AC-17, AC-20

10. SSA must implement an effective continuous monitoring strategy and program that must ensure the continued effectiveness of security controls by maintaining ongoing awareness of information security, vulnerabilities, and threats to the information system housing NDNH information. The continuous monitoring program must include configuration management, patch management, vulnerability management, risk assessments before making changes to the system and environment, ongoing security control assessments, and reports to 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 5, CA-7(1)(4); NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

11. SSA must maintain an asset inventory of all software and hardware components within the boundary of the information system housing NDNH information. The inventory must be detailed enough for 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 5, CM-2(3)(7), CM-7(1)(2)(4), CM-8(1)(3), CM-11, IA-3, PM-5, SA-4(1)(2)(9)(10), SC-17, SC-18, SI-4(2)(4)(5)

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

    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 5, PL-2, NIST SP 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*

13. SSA must 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 must 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 5, CA-5, NIST SP 800-18 Rev 1

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

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

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

15. SSA must limit and control logical and physical access to NDNH information to only those personnel authorized for such access based on their official duties, and identified in the records maintained by SSA pursuant to numbers 6 and 27 of this section. SSA must 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 5, AC-2, AC-3

16. SSA must transmit and store all NDNH information provided pursuant to this agreement in a manner that safeguards the information and prohibits unauthorized access. All electronic SSA transmissions of information to SSA and entities specified in the agreement must 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 140-3, *Security Requirements for Cryptographic Modules*; NIST SP 800-53 Rev 5, MP-4, SC-8

17. SSA must 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 140-3

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

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

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

19. SSA must prohibit remote access to NDNH information, except via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication. SSA must 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 140-3 NIST SP 800-53 Rev 5, AC-17, IA-2(6)(12), SC-8

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

    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 type of events. The audit trail system must protect data and the audit tool from addition, modification or deletion and should be regularly reviewed and analyzed for indications of inappropriate or unusual activity.

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

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

    OCSE does not extract information from the agency input files.

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

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

    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, NIST SP 800-53 Rev 5, AC-11, AC-12, AC-17, SC-10

23. SSA must 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, NIST SP 800-53 Rev 5, MP-4, MP-6, SI-12

24. When storage media are disposed of, the media will be destroyed or sanitized so that the erased records are not recoverable.

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

25. SSA must implement a Network Access Control (also known as Network Admission Control (NAC)) solution in conjunction with a Virtual Private Network (VPN) option to enforce security policy compliance on all SSA and non-SSA remote devices that attempt to gain access to, or use, NDNH information. SSA must use a NAC solution to authenticate, authorize, evaluate, and remediate remote wired and wireless users before they can access the network. The implemented NAC solution must evaluate whether remote machines are compliant with security policies through host(s) integrity tests against predefined templates, such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the SSA enterprise environment. SSA must disable functionality that allows automatic code execution. The solution must enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the 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 5, AC-17, AC-20, IA-2(6)(12), IA-3

26. SSA must ensure that the organization responsible for the data processing facility storing, transmitting, or processing NDNH information complies with the security requirements established in this security addendum. The "data processing facility" includes the personnel, facilities, documentation, data, electronic and 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 5, SA-9(2)

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

    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 5, PE-2, PE-3

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

    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 5, AC-2, PE-2

29. SSA must label printed reports containing NDNH information to denote the level of sensitivity of the information and limitations on distribution. SSA must maintain printed reports in a locked container when not in use and must 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 must 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 5, MP-2, MP-3, MP-4, MP-5, MP-6

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

    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 5, PE-3

I. CLOUD SOLUTION (OPTIONAL)

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

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

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

2. Use of a cloud solution must be approved in advance by OCSE at least 45 days before connectivity to FPLS information and confidential child support program information can be established. States that have already established a cloud solution housing FPLS information must send official notification of this major change to OCSE.

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

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

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

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

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

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

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

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

II. 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 must report confirmed and suspected incidents to OCSE using the security mailbox address: ocsesecurity@acf.hhs.gov. 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 A-130 – Appendix I; OMB M-17-12; NIST SP 800-53 Rev 5, IR-6

III. 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 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

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 February 25, 2022. OCSE considers this 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. SSA must provide a signed ATO letter whenever the ATO signature date on file with OCSE expires during this agreement. Failure to provide an updated ATO may result in the termination of 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 must demonstrate, and OCSE must 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 must be fully compliant with FISMA, OMB directives, and NIST guidelines.

Prior to receiving NDNH information, entities must 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 must first be granted the ATO through the authorization process according to NIST SP 800-37 Revision 2. In addition, if applicable, federal agencies that share NDNH information with entities specified in the agreement must 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 must have been conducted according to the NIST SP 800-37 Revision 2, as appropriate.

Federal agencies must comply with NIST SP 800-37 Revision 2, including implementing a continuous monitoring program for permitted entities. Agencies must 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 has 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-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy,* December 6, 2021.

IV. 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). OMB guidance provides that because 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-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy*, December 6, 2021

V. 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:

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

B. The SSA security contact is:

Jennifer Rutz, Director
Office of Information Security
Division of Compliance and Assessments
Suite 3208 Annex
601 Security Boulevard
Baltimore, MD 21235
Phone: (410) 966-8253
Email: Jennifer.Rutz@ssa.gov

VI. APPROVALS

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

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

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

Venkata Kondapolu -S Digitally signed by Venkata Kondapolu -S Date: 2022.11.14 09:30:00 -05'00'	
Venkata Kondapolu Director Division of Federal Systems Office of Child Support Enforcement	**Date**
Tanguler S. Gray -S Digitally signed by Tanguler S. Gray -S Date: 2022.11.14 22:23:28 -05'00'	
Tanguler Gray Commissioner Office of Child Support Enforcement	**Date**

B. Social Security Administration

Jennifer Rutz Digitally signed by Jennifer Rutz Date: 2022.11.30 10:17:44 -05'00'	
Jennifer Rutz Director Division of Compliance and Oversight Office of Information Security	**Date**
Michelle Christ Digitally signed by Michelle Christ Date: 2022.11.16 13:50:59 -05'00'	
Michelle L. Christ Acting Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	**Date**

APPENDIX A

Background: Prior Agreements

The data exchange operations governed by this agreement continues an existing matching program between the federal Office of Child Support Enforcement (OCSE) and the Social Security Administration (SSA). OCSE is required to provide SSA with information from the National Directory of New Hires (NDNH). Information exchanges have been ongoing for several years.

Prior information exchange agreements between the parties related to the DI Match are:

Computer Matching Agreement between Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match #1098/HHS #1506), "Title II-OCSE Quarterly Match Agreement," effective, December 17, 2015 through June 16, 2017. Recertification of the Computer Matching Agreement "Title II-OCSE Quarterly Match Agreement," (SSA Match #1098/HHS#1506), effective, June 17, 2017 through June 16, 2018.

Computer Matching Agreement between Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match #1098/HHS #1506), "Title II-OCSE Quarterly Match Agreement," effective, June 17, 2018 through December 16, 2019. Recertification of the Computer Matching Agreement "Title II-OCSE Quarterly Match Agreement," (SSA Match #1098/HHS#1801), effective, December 23, 2019 through December 22, 2020.

Computer Matching Agreement between Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match #1098/HHS #1506), "Title II-OCSE Quarterly Match Agreement," effective, June 17, 2018 through December 16, 2019. Recertification of the Computer Matching Agreement "Title II-OCSE Quarterly Match Agreement," (SSA Match #1098/HHS#2007), effective, December 23, 2020 through June 22, 2022.

APPENDIX B

DEFINITIONS
FOR
THE COMPUTER MATCHING AGREEMENT
BETWEEN
SSA AND OCSE

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

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 C

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

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 QW File: QW 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.	SSA claims personnel responsible for determining eligibility for DI	QW record identifier, name, SSN, processed date, address(es), wage amount, QW reporting period. Employer's name, transmitted agency code employer address(es).	National Directory of New Hires (NDNH) - QW File	42 U.S.C. § 653(j)(4)

Cost Benefit Analysis for the
Computer Matching Agreement (CMA)
between
Social Security Administration (SSA)
and
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 (QW) File)
SSA 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 QW File.

Background

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.

Subsequently, 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 QW information from OCSE for one or all of the following purposes: to establish or verify eligibility, continuing entitlement, and/or payment amounts of individuals under the DI program.

Methodology

In fiscal year (FY) 2021, SSA's Office of Research, Demonstration, and Employment Support (ORDES) and the Office of Disability Information Systems (ODIS) conducted a computer matching operation under CMA #1098. The system selected 118,993 cases using quarterly earnings data. Field office technicians further developed 20,810 of these cases. In this CBA report, SSA's Office of Data Exchange and International Agreements (ODXIA) examines the ORDES findings of the 20,810 cases that required additional development.

COSTS

The total FY 2021 personnel and computer costs for this matching operation are **$6,666,804.** **Key**

Element 1: Personnel Costs

For Agencies –

• Source Agency (OCSE) – reimbursed by SSA; included in SSA's costs
• Recipient Agency (SSA)

FO Development

For FY 2021, SSA's Office of Financial Policy and Operations (OFPO) reported a unit cost of $316.64 to conduct a Work CDR. Using $316.64 per case, the total development cost for the 20,810 CDRs developed during FY 2021 was **$6,589,278**.

• Justice Agency –N/A. SSA is unable to draw a direct correlation between the NDNH QW data received from OCSE in this matching program and *past* improper payments recovered through referrals to DOJ and Treasury for collection. Consequently, only costs and benefits associated with avoiding *future* improper payments (which does not entail referrals to DOJ and Treasury) are estimated in this cost-benefit analysis.

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) – reimbursed by SSA; included in SSA's costs
• Recipient Agency (SSA)

SSA's ODIS reports an FY 2021 estimated systems (computer) cost of **$42,526**.
• Justice Agencies -N/A. SSA is unable to draw a direct correlation between the NDNH QW data received from OCSE in this matching program and past improper payments recovered through referrals to DOJ and Treasury for collection. Consequently, only costs and benefits associated with avoiding future improper payments (which does not entail referrals to DOJ and Treasury) are estimated in this cost-benefit analysis.

Interagency Agreement Cost

For FY 2021, the total cost of the IAA for this matching operation is **$35,000**.

BENEFITS

Key Element 3: Avoidance of Future Improper Payments

To Agencies –

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

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

For FY 2021, the total benefits SSA realized from this matching operation is approximately **$104,190,336.**

Avoidance of future improper payments

Reduction of future monthly benefit payment amount

The systems selected approximately 118,993 CDR cases using quarterly earnings. Of these 118,993 cases, 10,728 cases resulted in termination of monthly benefit payments. The average monthly benefit payment amount was $1,214. The total adjustment in reduced monthly payment amount was $13,023,792. We conservatively predict that without this matching operation these incorrect payments would have continued for 8 months, costing SSA $104,190,336. Therefore, in FY21, we observed a savings of approximately **$104,190,336**.

• 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

We are unable to draw a direct correlation between the OCSE data and the recovery of retroactive improper payments. Therefore, we do not consider recovery of overpayments in the benefit calculations for this match.

• Justice Agencies – N/A

4
To Clients – N/A

To the General Public – N/A

Conclusion

For FY 2021, this matching operation resulted in an estimated overall savings of about **$104,190,336**. The total costs are approximately **$6,666,804**. These savings to the United States Treasury make this matching operation cost effective with a benefit to cost ratio of **15.6:1**; therefore, this match is cost effective. Accordingly, we recommend the continuance of this match.

CBA for the Quarterly Batch Matching Operation between SSA's MBR and CDR-CDD and OCSE's NDNH

Costs

Systems Costs	$42,526
Interagency Agreement (FY 2021)	$35,000
Field Office Alert Development Costs	$6,589,278
Total Costs	**$6,666,804**

Benefits

Terminated Monthly Payment Amount

Number of cases with Terminated Monthly Payment	10,278
Average Monthly Payment Amount	$1,214
Total Monthly Payment Amount	$13,023,792
Ongoing Monthly Payment (Projected 8 months)	$104,190,336
Total Benefits	**$104,190,336**
Benefit-to-Cost Ratio	**15.6:1**