

**COMPUTER MATCHING AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION
AND
THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES
OFFICE OF CHILD SUPPORT SERVICES**

“Title II-OCSS Quarterly Match Agreement”
SSA Match #1098/HHS Match #2505

I. PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

This computer matching agreement (agreement) governs a matching program between the Office of Child Support Services (OCSS) within the Administration for Children and Families (ACF), U.S. Department of Health and Human Services (HHS), and the Social Security Administration (SSA). The agreement covers the quarterly wage (QW) batch match for Title II Social Security Disability Insurance (SSDI). This agreement also governs the use, treatment, and safeguarding of the QW information exchanged. OCSS is the “source agency” and SSA is the “recipient agency,” as defined by the Privacy Act of 1974. 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 OCSS are executing this agreement to comply with the Privacy Act of 1974, as amended, and the regulations and guidance promulgated thereunder. SSA and OCSS 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, payment amounts, or all of the above, of individuals under the SSDI program.

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

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) 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 OCSS 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 system(s) of records notice(s) (SORN) 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, with limited exceptions at § 552a(u)(4)(B) and (C), that a Data Integrity Board (DIB) must 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.

Comparison of NDNH data with the specified SSA programs results in significant recovery of, or avoidance of, overpayments. For fiscal year (FY) 2023, the systems matched approximately 136,051 continuing disability review (CDR) cases using quarterly earnings. Of these 136,051 cases, 21,955 cases resulted in a cessation of monthly benefit payments. The average monthly benefit payment amount was \$1,231. It is conservatively predicted that without this matching operation these incorrect payments would have continued for eight months, costing SSA \$216,212,840. Therefore, in FY 2023, a savings of approximately \$216,212,840 was observed.

Details of the Cost Benefit Analysis 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. OMB issued implementing guidance to federal agencies in Part V of Appendix C of Circular A-123, *Requirements for Effective Estimation and Remediation of Improper Payments*, transmitted in OMB Memorandum M-18-20 (June 26, 2018), as modified by OMB Memorandum M-21-19 (March 5, 2021).

The NDNH is a national repository of new hire, QW, and Unemployment Insurance (UI) information that provides an effective, efficient, and comprehensive method of collecting and comparing information. SSA's use of NDNH QW information supports program accuracy, program administration, and reduces overpayments, securely and efficiently.

C. Specific Estimate of Any Savings

In addition to actual savings in section II.A. above and referenced in Appendix D, the benefit to the United States Treasury of this matching operation 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 (SOR)

The NDNH contains new hire and QW, and unemployment insurance information furnished by state and federal agencies on individuals and is maintained in the SOR "OCSS National Directory of New Hires," System No. 09-80-0381; see System of Records Notice (SORN) published in full at 89 Fed. Reg. 25625 (April 11, 2024). The disclosure of NDNH information by OCSS to SSA constitutes a "routine use," as defined by the Privacy Act. 5 U.S.C. § 552a(b)(3). Routine use number 9 of the NDNH SORN authorizes the disclosure of NDNH records to SSA for purpose of verifying eligibility for Social Security Administration's programs and the administration of such programs, and for the administration of the Ticket to Work program.

SSA's relevant SORs are the Master Beneficiary Record (MBR), System No. 60-0090 SORN published in full at 71 Fed. Reg. 1826 (January 11, 2006), and amended at 72 Fed. Reg. 69723 (December 10, 2007), 78 Fed. Reg. 40542 (July 5, 2013), 83 Fed. Reg. 31250-31251 (July 3, 2018), 83 Fed. Reg. 54969 (November 1, 2018), 89 Fed. Reg. 825 (January 5, 2024), and 89 Fed. Reg. 14554 (February 27, 2024); the Completed Determination Record (CDR)-Continuing Disability Determinations (CDD) file, System No. 60-0050, published in full at 71 Fed. Reg. 1813 (January 11, 2006), and amended at 72 Fed. Reg. 69723 (December 10, 2007), 83 Fed. Reg. 54969 (November 1, 2018), 84 Fed. Reg. 17907 (April 26, 2019), and 89 Fed. Reg. 825 (January 5, 2024).

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

The information in these SORs may be updated during the effective period of this agreement as required by the Privacy Act. The SORNs involved in this computer matching program have routine uses permitting the disclosures needed to conduct this match.

B. Number of Records Involved

Each SSA finder file will contain approximately 13 million records of individuals.

The NDNH contains approximately 1.6 billion new hire, QW, and UI 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 OCSS 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 OCSS the following data elements in the finder file:

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

2. OCSS 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

OCSS Responsibilities

1. On a quarterly basis, OCSS will compare the SSA finder file against the QW files in the NDNH for the purpose set forth in this agreement.
2. OCSS 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 SSDI beneficiaries for comparison by OCSS against the QW files in the NDNH.
2. SSA will use the QW information to administer the SSDI 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 required under 5 U.S.C. § 552a(e)(12).

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 SSDI applicants or beneficiaries with the NDNH database no more frequently than quarterly. OCSS may commence comparisons and disclosures under this agreement upon completion of all of the following requirements:

- OCSS and SSA agency officials sign the agreement;
- SSA submits the documentation required by OCSS to assess the security posture of the agency; and
- SSA, as the recipient agency, completes the notice and reporting requirements specified in sections IV. and 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). Accordingly, SSA will provide the following notices, respectively, to persons whose records are disclosed from the SORs involved in the matching program established under this agreement.

1. Notice to Applicants

SSA will notify individuals at the time of application for SSDI benefits regarding the comparison of his or her records against those of other agencies to verify his or her 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 SSDI 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 his or her eligibility or payment amounts. SSA includes notice to SSDI beneficiaries in mailings pertaining to work CDRs (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 has independently verified the information;
2. 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;

3. 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
4. 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 OCSS are correct and will make the necessary adjustment to the SSDI benefit.

SSA will not take any action against a beneficiary solely because of the findings from this matching program.

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, OCSS and SSA must destroy the records, in accordance with the security addendum herein, including the erasure of all electronic records.

A. SSA Records in the Input File

OCSS 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 OCSS.

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 required to support the matching program and will then destroy the records. SSA will not duplicate or disseminate NDNH information within or outside SSA without the written permission of OCSS except as necessary within SSA for ongoing operations of the matching program or for the purpose of disaster recovery. OCSS 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 required for any processing related to the SSDI 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 OCSS under this agreement in accordance with the applicable Federal Records Retention Schedule. 44 U.S.C. Chapter 33.

Neither SSA nor OCSS 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 OCSS will keep an accurate accounting of disclosures from an individual's records, as required by subsection (c) of the Privacy Act, 5 U.S.C. § 552a(c).

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).

This section of the agreement and the security addendum specify procedures for ensuring the security of the records used in the matching program.

NDNH comparison results must be safeguarded, whether labeled as NDNH information or commingled with other information and, if an agency commingles NDNH information, the agency must ensure that computer matching agreement requirements and conditions apply to all information with which NDNH information is maintained.

SSA and OCSS will comply with the requirements of the Privacy Act, the Computer Matching and Privacy Protection Act, the Federal Information Security Management Act of 2002, as amended by the Federal Information Security and Modernization Act of 2014, 44 U.S.C. § 3551 et seq.; related OMB circulars and memoranda, such as Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016), and M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017); National Institute of Standards and Technology (NIST) guidance; and the Federal Acquisition Regulations. These laws, regulations, and other authorities include requirements for safeguarding and limiting access to 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 applicable laws, regulations, NIST standards, and OMB directives, including those published subsequent to the effective date of this agreement.

FISMA requirements apply to all federal employees, 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 must be taken and considered as part of this agreement, as if the provisions contained in the addendum were fully set forth here.

A. Breach Reporting

If either SSA or OCSS experiences a suspected or confirmed incident involving the breach (i.e., loss) of PII provided by SSA or OCSS under the terms of this agreement, they will follow the reporting guidelines issued by OMB. In the event of a suspected or confirmed PII breach, the agency experiencing the breach is responsible for following its established procedures, including notification to the proper organizations. In addition, the agency experiencing the suspected or confirmed breach will notify the other agency's point of contact named in this agreement. If OCSS is unable to speak with the SSA Privacy and Disclosure Policy Breach Contact within one hour or if for some other reason notifying the SSA Privacy and Disclosure Policy Breach Contact is not practicable (e.g., it is outside of the normal business hours), OCSS will call SSA's Enterprise-IT Customer Service Desk at (877) 697-4889. SSA will notify the OCSS Security team (OCSSSecurity@acf.hhs.gov) of all suspected or confirmed breaches within one hour. If SSA is unable to speak with OCSS' Systems Security Contact within one hour, SSA will contact the OCSS Director of Operations at (877) 697-4889.

B. Breach Notification

SSA and OCSS will follow PII breach notification policies and related procedures issued by OMB. If the agency that experiences 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 OCSS 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 his or her official duties in connection with the uses of the data authorized in this agreement. Further, SSA and OCSS 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 OCSS 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 (e.g., door locks, card keys, biometric identifiers, etc.). Only authorized personnel will transmit the data matched and any data created by the match. SSA and OCSS will establish appropriate safeguards for such data, as determined by a risk-based assessment for the circumstances involved.

E. Technical Safeguards

SSA and OCSS 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 OCSS will strictly limit authorization to those electronic data areas necessary for authorized personnel to perform his or her official duties.

F. Application of Policy and Procedures

SSA and OCSS shall adopt and adhere to policies and procedures that ensure the user of information contained in their respective records, or obtained from one another, is strictly limited to the purposes outlined in this agreement. Access to NDNH records shall be restricted to agency officers and employees with a demonstrated need to perform official duties, in accordance with 5 U.S.C. § 552a(b)(1). Prior to accessing any records, agencies must enforce all applicable protocols, including privacy policies, system access controls, and training requirements. Authorized users must complete all mandated privacy and security trainings and sign the requisite rules of behavior. SSA and OCSS 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 Rev. 2, 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).

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

1. OCSS will not duplicate or disseminate SSA finder files, the information contained therein, and the information submitted within or outside OCSS without the written approval of SSA, except as necessary within OCSS 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. OCSS will handle the files as provided in section VI once the matching activity authorized under this agreement is completed.
2. OCSS will use and access the SSA finder files and information provided by SSA only for the purposes specified in this agreement.
3. OCSS 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 OCSS 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 OCSS, 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. OCSS will not grant such authority unless the disclosure is required by law or is essential to the matching program.
4. Information provided by OCSS remains the property of OCSS. SSA will handle the files and records 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 United 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. OCSS verifies the accuracy of name and SSN combinations maintained by OCSS 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 SSN combinations contained in the new hire file and the UI file against which input files are compared have been verified against SSA databases. For QW, 77 percent of name and SSN 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 2022 Title II Payment Accuracy Report, August 2023), 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). OCSS 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 OCSS to incur obligations through the performance of services described herein. The authority to perform such services requires the execution of an OCSS Reimbursement Agreement (RA) and Fiscal Service (FS) Forms 7600A and 7600B. OCSS may incur obligations by performing services under this agreement only on a fiscal year basis. The 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 OCSS. Since OCSS' performance under this agreement spans multiple fiscal years, SSA will prepare FS Forms 7600A and 7600B at the beginning of each succeeding fiscal year during which OCSS 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 fiscal year. OCSS' 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 OCSS must reimburse OCSS for costs incurred in furnishing the information, at rates which OCSS determines to be reasonable. 42 U.S.C. § 653(k)(3).

SSA will reimburse OCSS for use of NDNH information on a quarterly basis. SSA will reimburse OCSS via the following:

- a Reimbursable Agreement (RA), prepared by OCSS; and
- FS Forms 7600A and 7600B prepared by SSA in Treasury's G-Invoicing system.

The RA and FS Forms 7600A and 7600B will be entered into each fiscal year and will address costs and reimbursement terms. OCSS and SSA must sign all documents. SSA may incur obligations only on a fiscal year basis. SSA's ability to reimburse OCSS in fiscal years beyond FY 2024 is subject to the availability of funds.

OCSS will collect funds from SSA in FY 2026 and beyond through Treasury's G-Invoicing system, which will generate an Intra-Governmental Payment and Collection (IPAC) sufficient to reimburse OCSS for the costs it has incurred for performing services through the date of billing. OCSS 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 OCSS 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 OCSS will sign FS Forms 7600A and 7600B and an OCSS RA 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 OCSS intend that the effective date of this agreement will be December 23, 2025, the day after the expiration date of the existing matching agreement, HHS DIB, SSA Match #1098/HHS #2302, which was amended and renewed through December 22, 2025.

B. Modification of the Agreement

This agreement may be modified at any time by a written amendment approved by SSA and OCSS. The proposed modification must be reviewed by HHS and SSA DIB counsel to determine if the change is significant and requires a new agreement. The parties must sign modified FS Forms 7600A and 7600B if actual costs exceed the estimated cost.

C. Termination of the Agreement

Prior to the agreement's end in accord with this section, the agreement may be terminated in one of 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 OCSS under section 453(k) of the Act as agreed upon in section XI of this agreement and the fiscal agreements of both SSA and OCSS or OCSS 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 OCSS 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 Information Technology Dashboard, the Annual Report to Congress, and the Major IT Business Case. OCSS is required to provide performance measures demonstrating how the FPLS supports OCSS' strategic mission, goals and objectives, and cross-agency collaboration. OCSS also requests such performance reporting to ensure matching partners use NDNH information for the authorized purpose.

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

The performance reports may also assist in the development of a cost benefit analysis of the matching program required for any subsequent matching agreements in accordance with 5 U.S.C. § 552a(o)(1)(B). See section II.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 Services contacts for programs and security are:

Angela Kasey-Henry, Data Access Federal Oversight Manager
Division of Federal Systems
Office of Child Support Services
Administration for Children and Families
Mary E. Switzer Building
330 C Street, SW
Washington, DC 20201
Telephone: (202) 260-4712
Email: Angela.Kasey-Henry@acf.hhs.gov

System Security Issues

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

B. Incident Reporting contact information for the U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Services is:

Venkata Kondapolu
Phone: (202) 401-9389, option #3
Email: ocsssecurity@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
Telephone: (410) 965-3353
Email: Kristine.Erwin-Tribbitt@ssa.gov

Systems Issues

Mary Lindauer, Branch Chief
Disability Review and Work Incentives Branch
Division of Disability Online Access and Analysis
Social Security Administration
3604-RMB Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Telephone: (410) 966-6581
Email: Mary.D.Lindauer@ssa.gov

Matching Agreement Issues

Sonia Robinson, Government Information Specialist
Privacy and Disclosure Policy
Law and Policy
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235-6401
Telephone: (410) 966-4115
Email: Sonia.V.Robinson@ssa.gov

Data Exchange Issues

Jamillah Jackson, Branch Chief
Federal Agreements Branch
Office of Income Security Programs
Law and Policy
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235-6401
Telephone: (410) 9653747
Email: Jamillah.N.Jackson@ssa.gov

Systems Security

Robert Muffoletto, Division Director
Division of Compliance and Assessments
Information Security
Chief Information Officer
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235
Telephone: (410) 966-5248
Email: Robert.Muffoletto@ssa.gov;
SOC@ssa.gov

Breach Contact

Andrea Huseth, Division Director
Electronic Interchange, Liaison, and Breach Division
Privacy and Disclosure Policy
Law and Policy
Social Security Administration
6401 Security Boulevard, G-401 WHR
Baltimore, MD 21235
Telephone: (410) 608-9675
Email: Andrea.Huseth@ssa.gov

XVI. INTEGRATION CLAUSE

This agreement, the Security Addendum, the appendices, FS Forms 7600A and 7600B, and the OCSS RA 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. AUTHORIZED SIGNATURES

By his or her signatures below, the authorized officials approve this agreement.

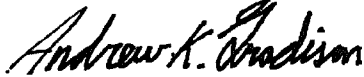
The authorized program officials whose signatures appear below accept and expressly agree to the terms and conditions expressed herein, confirm that no verbal agreements of any kind will be binding or recognized, and hereby commit his or her respective organizations to the terms of this agreement.

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

U.S. Department of Health and Human Services

LINDA A. BOYER -S Digitally signed by LINDA A. BOYER -S Date: 2025.09.22 08:09:12 -04'00'	
Linda Boyer Deputy Commissioner Office of Child Support Services	Date

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


	
Andrew Gradison Acting Assistant Secretary Administration of Children and Families	Date

Social Security Administration


Jennifer Karangelen Digitally signed by Jennifer Karangelen Date: 2025.09.12 10:55:14 -04'00'	
Jennifer Karangelen Acting Deputy Executive Director Privacy and Disclosure Policy Law and Policy	Date

A. Data Integrity Boards

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

 <small>Clark Minor (Oct 6, 2025 11:33:41 EDT)</small>	
Clark Minor Chairperson HHS Data Integrity Board U.S. Department of Health and Human Services	Date

Social Security Administration Data Integrity Board

	
Matthew D. Ramsey Chair SSA Data Integrity Board Social Security Administration	Date OCT 7, 2025

SECURITY ADDENDUM

**U.S. Department of Health and Human Services
Administration for Children and Families
Office of Child Support Services
and
The Social Security Administration**

Title II-OCSS Quarterly Match Agreement
SSA Match #1098/HHS Match #2505

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 Services (OCSS) 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, OCSS and SSA agree to comply with the provisions of the Social Security Act (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. OCSS 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, OCSS 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 and physical records, other machine-readable information, and the information systems of OCSS and SSA and SSA authorized entities specified in the agreement which are hereinafter “OCSS” and “SSA.”

III. SECURITY AND PRIVACY SAFEGUARDING REQUIREMENTS

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

This section provides the safeguarding requirements which OCSS 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 and the safeguards in place at OCSS 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 his or her official duties in connection with the authorized purposes specified in the agreement.

OCSS restricts access to, and disclosure of, the agency input files to authorized personnel who need them to perform his or her 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*, Access Control (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.

OCSS 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, Planning (PL)-4(1), Personnel Security (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).

OCSS 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; HHS-OCIO-OIS-2020-02-002; 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 in 5 U.S.C. § 552a, and the federal laws governing use and misuse of NDNH information.

OCSS 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, Awareness and Training (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.

OCSS 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 OCSS upon request.

OCSS 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 PII) 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, in either electronic or physical form, to OCSS, as designated in this security addendum. The requirement for SSA to report confirmed or suspected incidents involving NDNH information to OCSS exists in addition to, not in lieu of, any SSA requirements to report to the Cybersecurity and Infrastructure Security Agency (CISA) or other reporting agencies.

OCSS 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, OCSS will report confirmed and suspected incidents to the SSA security contact designated in this security addendum. The requirement for OCSS to report confirmed or suspected incidents to SSA exists in addition to, not in lieu of, requirements to report to CISA or other reporting agencies.

Policy/Requirements Traceability: OMB Circular A-130 – Appendix I; OMB M-17-12; HHS-OCIO-PIM-2020-05-003; NIST SP 800-53 Rev. 5, Incident Response (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.

OCSS 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 140-3 encryption standards. Personally owned devices must not be authorized. See numbers 8 and 19 of this section for additional information.

OCSS 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.

OCSS 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.

OCSS 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, Configuration Management (CM)-2(3)(7), CM-7(1)(2)(4), CM-8(1)(3), CM-11, Identification and Authentication (IA)-3, Program Management (PM)-5, System and Services Acquisition (SA)-4(1)(2)(9)(10), System and Communications Protection (SC)-17, SC-18, System and Information Integrity (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.

OCSS 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.

OCSS 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. OCSS 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.

OCSS 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 his or her official duties, and identified in the records maintained by SSA under numbers 6 and 27 of this section.

SSA must prevent personnel from browsing by using technical controls or other compensating controls.

OCSS limits and controls logical and physical access to the agency input files to only those personnel authorized for such access based on his or her official duties. OCSS 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 under 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 140-3 compliant product.

SSA and OCSS exchange data via a mutually approved and secured data transfer method that utilizes a FIPS 140-3 compliant product.

Policy/Requirements Traceability: OMB M-17-12; FIPS 140-3, *Security Requirements for Cryptographic Modules*; NIST SP 800-53 Rev. 5, Media Protection (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 140-3 compliant product. See numbers 8 and 18 of this section for additional information.

OCSS 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.

OCSS 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 140-3 compliant) transmission link and using two-factor authentication. SSA must control remote access through a limited number of managed access control points.

OCSS prohibits remote access to the agency input files except via a secure and encrypted (FIPS 140-3 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 must be regularly reviewed and analyzed for indications of inappropriate or unusual activity.

OCSS 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 must be regularly reviewed and analyzed for indications of inappropriate or unusual activity.

Policy/Requirements Traceability: NIST SP 800-53 Rev. 5, Audit and Accountability (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 OCSS written approval. SSA must comply with the retention and disposition requirements in the agreement.

OCSS 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.

OCSS 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.

OCSS 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. All parties agree that 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 remedy 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.

OCSS 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.

OCSS 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 under 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.

OCSS stores the agency input files provided under 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, Physical and Environment Protection (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.

OCSS maintains lists of personnel authorized to access facilities and systems processing the agency input files. OCSS 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.

OCSS 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.

OCSS 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

IV. 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 OCSS 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 OCSS.
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 compliant with NIST guidelines.
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, and the data retention policies agreed upon by SSA and OCSS to ensure that all required statutory requirements are met. 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.

V. BREACH REPORTING AND NOTIFICATION RESPONSIBILITY

Upon disclosure of NDNH information from OCSS 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, in either electronic or physical form, to the OCSS security team. Incident reporting contact information is contained in section VIII of this security addendum. SSA is responsible for all reporting and notification activities, including but not limited to: investigating the incident; communication with Cybersecurity and Infrastructure Security Agency (CISA); notifying individual 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.

OCSS has appropriate procedures in place to report security and privacy incidents, or suspected incidents involving the SSA finder files. Immediately upon discovery but in no case later than one hour after discovery of the incident, OCSS will report confirmed or suspected incidents to the SSA security contact designated in this security addendum (see section VIII.). If OCSS is unable to speak with the SSA security contact is not practicable (e.g., it is outside of the normal business hours), OCSS will call SSA's Enterprise-IT Customer Service Desk at (877) 697-4889. The requirement for OCSS to report confirmed or suspected incidents to SSA exists in addition to, not in lieu of, requirements to report to CISA or other reporting agencies.

Policy/Requirements Traceability: CISA *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

VI. SECURITY AUTHORIZATION

OCSS requires systems that process, transmit, or store NDNH information to be granted authorization to operate following the guidelines in NIST 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

A. SSA Security Posture

OCSS 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.

An ATO serves as an attestation that security is adequately integrated into the system and remains persistent throughout the approval timeline via technical, management, and continuous monitoring controls. The ATO also affirms SSA will conclude remediation of vulnerabilities addressed in a Plan of Actions and Milestones (POA&Ms). To illustrate the scope of these requirements, SSA has provided evidence to support the implementation of the following controls across the technical, management, and continuous monitoring domains:

Technical Controls Summary

- Access Control
- Data Encryption
- Security Software
- Configuration Management

Management Controls Summary

- Security Policy
- Risk Management
- Training and Awareness
- Monitoring and Logging
- Incident Response

Continuous Monitoring Controls Summary

- Identification and Remediation of new vulnerabilities
- Plan of Action and Milestone (POA&M) remediation

The SSA provisional ATO for the Electronic Disability Mainframe system (eDIB MF) was signed on 2/04/2025. OCSS considers this evidence that the SSA environment complies with the security requirements in this security addendum (which include technical, management and continuous monitoring controls applied and maintained throughout the ATO period).

The effective period for an ATO is three years. SSA must provide a signed ATO letter whenever the ATO signature date on file with OCSS expires during this agreement. Failure to provide an updated ATO may result in the termination of this agreement. Additionally, OCSS reserves the

right to verify if compensating controls, updated vulnerability remediation results, and updated POA&Ms meet the SSA standard during the agreement period of the ATO. Failure to meet the required objectives may result in suspension of data flow until compliance with all stated objectives of the ATO are completed.

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

B. SSA Permitted Entity Security Posture

Prior to the redisclosure of NDNH information by SSA to any authorized entity, SSA must demonstrate, and OCSS 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 Rev. 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 Rev. 2, as appropriate.

Federal agencies must comply with NIST SP 800-37 Rev. 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-25-04, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, January 15, 2025.

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 OMB 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(1)(2) of the Social Security Act. 42 U.S.C § 653(1)(2) and 5 U.S.C. § 552a(e)(10).

Policy/Requirements Traceability: OMB M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, January 15, 2025; OMB Circular No. A-130, Appendix I.

VIII. PERSONS TO CONTACT

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

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

- B. Incident Reporting contact information for the U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Services is:

Venkata Kondapolu
Phone: (202) 401-9389, option #3
Email: ocsssecurity@acf.hhs.gov

- C. The SSA security contact is:

Robert Muffoletto, Division Director
Division of Compliance and Assessments
Information Security
Chief Information Officer
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 966-5248
Email: Robert.Muffoletto@ssa.gov; SOC@ssa.gov

Breach Contact

Andrea Huseh, Division Director
Electronic Interchange, Liaison, and Breach Division
Privacy and Disclosure Policy
Law and Policy
Social Security Administration
6401 Security Boulevard, G-401 WHR
Baltimore, MD 21235
Telephone: (410) 608-9675
Email: Andrea.Huseh@ssa.gov

IX. AUTHORIZED SIGNATURES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this agreement.

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. By signing this document electronically, the signatories agree 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

Venkata Kondapolu -S Digitally signed by Venkata Kondapolu -S Date: 2025.09.19 09:39:53 -04'00'	
Venkata Kondapolu Director Division of Federal Systems Office of Child Support Services	Date
LINDA A. BOYER -S Digitally signed by LINDA A. BOYER -S Date: 2025.09.22 08:09:47 -04'00'	
Linda Boyer Deputy Commissioner Office of Child Support Services	Date

B. Social Security Administration

<i>Robert Muffoletto</i>	
Robert Muffoletto Division Director Division of Compliance and Assessments Information Security Chief Information Officer	Date 09/12/2025
Jennifer Karangelen	Digitally signed by Jennifer Karangelen Date: 2025.09.12 10:55:57 -04'00'
Jennifer Karangelen Acting Deputy Executive Director Privacy and Disclosure Policy Law and Policy	Date

APPENDIX A

Background: Prior Agreements

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

Prior data matching agreements between the parties related to the SSDI Match are:

Computer Matching Agreement between SSA and OCSS, Administration for Children and Families (ACF), Department of Health and Human Services (HHS) (SSA Match #1098/HHS #1506), "Title II-OCSS Quarterly Match Agreement," effective, December 17, 2015 through June 16, 2017. Renewal of the Computer Matching Agreement "Title II-OCSS Quarterly Match Agreement," (SSA Match #1098/HHS#1506), effective, June 17, 2017 through June 16, 2018.

Computer Matching Agreement between SSA and OCSS, ACF, HHS (SSA Match #1098/HHS #1801), "Title II-OCSS Quarterly Match Agreement," effective, June 17, 2018 through December 16, 2019. Renewal of the Computer Matching Agreement "Title II-OCSS Quarterly Match Agreement," (SSA Match #1098/HHS#1801), effective, December 23, 2019 through December 22, 2020.

Computer Matching Agreement between SSA and OCSS, ACF, HHS (SSA Match #1098/HHS #2007), "Title II-OCSS Quarterly Match Agreement," effective, June 17, 2018 through December 16, 2019. Renewal of the Computer Matching Agreement "Title II-OCSS Quarterly Match Agreement," (SSA Match #1098/HHS#2007), effective, June 22, 2022 through June 21, 2023.

Computer Matching Agreement between SSA and OCSS, ACF, HHS (SSA Match #1098/HHS #2302), "Title II-OCSS Quarterly Match Agreement," effective, June 23, 2023 through December 22, 2024. Renewal of the Computer Matching Agreement "Title II-OCSS Quarterly Match Agreement," (SSA Match #1098/HHS#2007), effective, December 23, 2024 through December 22, 2025.

APPENDIX B
DEFINITIONS
FOR
THE COMPUTER MATCHING AGREEMENT
BETWEEN
SSA AND OCSS

“Title II-OCSS Quarterly Match Agreement”
SSA Match #1098/HHS Match #2505

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 Supplemental Security Income beneficiaries receiving a disability-related benefit including Ticket-to-Work program beneficiaries.

“**Disclose**” and “**disclosure**” mean the release of information or data by either SSA or OCSS, 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 U.S. territories.

APPENDIX C

Business Needs Assessment Chart for the Agreement between SSA and OCSS Covering the Title II NDNH Quarterly Batch SSA Match #1098/HHS Match #2505

SSA Application	Match Method	Function	Elements Provided by SSA to Conduct Match	Elements Provided by OCSS to Conduct Match	SSA User	Elements temporarily displayed if a match is found	OCSS 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 SSDI 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 SSDI	QW record identifier, name, SSN, processed date, address(es), wage amount, QW reporting period. Employer's name, transmitter agency code, employer address(es).	National Directory of New Hires (NDNH) - QW File	42 U.S.C. § 653(j)(4)

APPENDIX D

**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 Services (OCSS)**

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

Objective

The purpose of this cost benefit analysis (CBA) is to determine the cost-effectiveness of the matching operation between SSA's MBR and CDR-CDD and OCSS' NDNH QW File.

Background

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

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

Methodology

In fiscal year (FY) 2023, the 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 136,051 cases using quarterly earnings data. Field office technicians further developed 31,491 of these cases. In this CBA report, the Office of Data Exchange and International Agreements (ODXIA) examines the ORDES findings of the 31,491 cases that required additional development.

COSTS

The total FY 2023 personnel and computer costs for this matching operation are **\$10,902,712**.

Key Element 1: Personnel Costs

For Agencies –

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

FO Development

For FY 2023, the Office of Financial Policy and Operations (OFPO) reported a unit cost of \$343.88 to conduct a Work CDR. Using \$343.88 per case, the total development cost for the 31,491 CDRs developed during FY 2023 was **\$10,829,125**.

- 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 (OCSS) – N/A
- Recipient Agency (SSA)

ODIS reports an FY 2023 estimated systems (computer) cost of **\$38,587**.

- Justice Agencies -N/A.

Interagency Agreement Cost

For FY 2023, the total cost of the interagency agreement for this matching operation is **\$35,000**.

BENEFITS

Key Element 3: Avoidance of Future Improper Payments

To Agencies –

- Source Agency (OCSS)
- 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 2023, the total benefits SSA realized from this matching operation is approximately **\$216,212,840**.

Avoidance of future improper payments

Termination of future monthly benefit payment amount

The systems selected approximately 136,051 CDR cases using quarterly earnings. Of these 136,051 cases, 21,955 cases resulted in termination of monthly benefit payments. The average monthly benefit payment amount was \$1,231. The total adjustment in terminated monthly payment amount was \$27,026,605. We conservatively predict that without this matching operation these incorrect payments would have continued for 8 months, costing SSA \$216,212,840. Therefore, in FY23, we observed a savings of approximately **\$216,212,840**.

- 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 (OCSS) – N/A
- Recipient Agency (SSA)

Recovery of improper payments and debts

We are unable to draw a direct correlation between the OCSS 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

To Clients – N/A

To the General Public – N/A

Conclusion

For FY 2023, this matching operation resulted in an estimated overall savings of about **\$216,212,840**. The total costs are approximately **\$10,902,712**. These savings to the United States Treasury make this matching operation cost effective with a benefit to cost ratio of **19.8:1**; therefore, this match is cost effective. Accordingly, we recommend the continuance of this match.

**Cost Benefit Analysis for the Quarterly Batch Matching Operation
between SSA's MBR and CDR-CDD and OCSS's NDNH**

Costs

Systems Costs	\$38,587
Interagency Agreement (FY 2023)	\$35,000
Field Office Alert Development Costs	\$10,829,125
Total Costs	\$10,902,712

Benefits

Terminated Monthly Payment Amount

Number of cases with Terminated Monthly Payment	21,955
Average Monthly Payment Amount	\$1,231
Total Monthly Payment Amount	\$27,026,605
Ongoing Monthly Payment (Projected 8 months)	\$216,212,840
Total Benefits	\$216,212,840

Benefit-to-Cost Ratio	19.8:1
------------------------------	---------------