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

Verification of Eligibility for Extra Help (Low Income Subsidy)
under the Medicare Part D Prescription Drug Coverage Program
SSA Match # 1306/HHS Match # 2501

I.   PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

A. Purpose of the Matching Agreement

This computer matching agreement, herein after "agreement" governs a matching program between the Office of Child Support Services (OCSS) and the Social Security Administration (SSA). OCSS will provide SSA with quarterly wage (QW) and unemployment insurance (UI) information from the National Directory of New Hires (NDNH) to assist SSA in determining eligibility of applicants for Extra Help (low-income subsidy assistance) under the Medicare Prescription Drug, Improvement, and Modernization Act (MMA) of 2003 (Pub. L. 108-173) (Extra Help). This agreement also governs the use, treatment, and safeguarding of the information exchanged. OCSS is the "source agency" and SSA is the "recipient agency," as defined by the Privacy Act.
5 U.S.C. §§ 552a(a)(9) and (11).

This matching program assists SSA in: (1) determining eligibility of applicants for Extra Help; (2) redetermining eligibility of existing Extra Help beneficiaries during periodic screening; and (3) administering the Extra Help program.

A computerized comparison of two systems of records (SORs) for the purpose of establishing or verifying the eligibility for benefits, or continuing compliance with statutory and regulatory requirements, by applicants for or recipients or beneficiaries of cash or in-kind assistance or payments under a federal benefit program constitutes a "matching program," as defined by the Privacy Act.
5 U.S.C. § 552a(a)(8)(A)(i)(I)

The Privacy Act provides that no record contained in a 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 and the regulations and guidance promulgated thereunder. OCSS and SSA have been parties to matching agreements for this purpose since April 1, 2005. Appendix A provides background information about these prior agreements.

The SSA component responsible for this agreement and its contents is the Office of Privacy and Disclosure. 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 NDNH information. Personnel are defined as employees, contractors, or agents of OCSS and SSA.

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. Subsection 453(j)(4) of the Act provides that OCSS shall provide the Commissioner of SSA with all information in the NDNH. 42 U.S.C. § 653(j)(4). SSA has authority to use the data to determine entitlement to and eligibility for programs it administers (*see sections* 1631(e)(1)(B) and(f), and 1860D-14(a)(3) of the Act, codified at 42 U.S.C. §§ 1383(e)(1)(B) and (f), and 1395w-114(a)(3)). Disclosures under this agreement are authorized by routine uses published in each agency's applicable System of Records Notice pursuant to 5 U.S.C. §552a(b)(3) (the applicable System of Records Notices (SORNs) and routine uses are identified in Section III.A., below).

The Act provides that the determination of whether a Part D eligible individual residing in a state is a subsidy eligible individual shall be determined under the state plan for medical assistance or by the Commissioner of Social Security. 42 U.S.C. § 1395w- 114(a)(3)(B)(i).

SSA has independent authority to collect this information regarding Medicare Parts A-D eligibility and premium calculations via sections 202-205, 223, 226, 228, 1611, 1631, 1818, 1836, 1839, 1840, and 1860D-1 to 1860D-15 of the Act (42 U.S.C. §§ 402-405, 423, 426, 428, 1382, 1383, 1395i-2, 1395o, 1395r, 1395s, and 1395w-101 to 1395w-115).

C. Definitions

See Appendix B.

II. JUSTIFICATION AND 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

Unless statutorily excepted or waived by both agencies' Data Integrity Boards (DIBs), a cost benefit analysis must be completed and submitted to the DIBs to consider in determining whether to approve the matching program. 5 U.S.C. § 552a(u)(4)(A). If the analysis does not demonstrate that the matching program is likely to be cost effective, the DIBs may approve the matching agreement based on other supporting justifications. *See* OMB guidance in *Privacy Act of 1974: Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1998*, 54 Federal Register (Fed. Reg.) 25818 (June 19, 1989), at pages 25821 and 25828-25829. *See Appendix C.*

The cost benefit analysis prepared by SSA for this agreement, included at Appendix C, does not quantify any improper payments avoided or recovered in Key Elements 3 and 4 to offset against the costs of conducting the matching program estimated in Key Elements 1 and 2. As a result, it fails to demonstrate that the matching program is likely to be cost-effective, based on HHS' interpretation of the term "demonstrate" in 5 U.S.C. § 552a(u)(4)(A).

The benefit of conducting this matching operation is the increased accuracy of SSA subsidy determinations, and the cost-savings gained by reducing the need for manual verifications of all income and resource allegations on Medicare Part D subsidy initial and redetermination applications.

B. Other Supporting Justifications

Computer matching is the most efficient and impartial method whereby SSA can, as required by those authorities, obtain and use data from other federal and state agency sources (including the NDNH data that 42 U.S.C. § 653(j)(4) requires OCSS to give SSA) to verify the data that applicants and beneficiaries give SSA, to determine the applicants' and beneficiaries' entitlement to and eligibility for programs SSA administers (including the Extra Help program).

The matching program expedites the Extra Help program enrollment process and reduces the enrollment burden for Medicare beneficiaries. Additionally, computer matching ensures a correct Extra Help program eligibility determination while reducing the level of effort that SSA Field Offices (FO) must expend to manually verify all income and resource allegations on the initial Extra Help application and during subsequent eligibility redeterminations. FOs perform fewer manual verifications when computerized data exchanges verify alleged income. Appendix D outlines the business need for this data exchange.

SSA benefits from administrative savings by avoiding the cost of manual development of income and resources reported on initial and redetermination applications. SSA estimates that the benefit-to-cost ratio for this matching operation is 25.9:1.

The NDNH is the only nationally centralized directory of new hire, QW, and UI information and, as such, provides an effective, efficient, and comprehensive method of collecting and comparing this information. SSA's use of NDNH information supports program accuracy, program administration, and potentially reduces overpayments (albeit, the amount of overpayments avoided has not been quantified at this time). SSA uses NDNH information to verify an individual's statement of income and resources, as attested to by the individual under the Extra Help program. Applicants must make attestations under penalty of perjury and SSA is responsible for verifying applicants' income and resource allegations.

There is no other administrative activity that can accomplish the same purpose and provide the same security safeguards with the same degree of efficiency and accuracy.

C. Specific Estimate of Any Savings

The benefit to SSA of conducting this matching operation is cost savings or cost avoided, and, potentially, improper payments avoided and/or recovered in excess of costs incurred. The costs savings result from the fact that computer matching increases the efficiency and accuracy of SSA subsidy determinations and reduces the need for manual verifications by Field Offices (FO) of all income and resource allocations on Medicare Part D subsidy initial and redetermination applications.

For fiscal year (FY) 2023, SSA's Office of Public Service and Operations Support reported an average development time of 21 minutes for initial applications and 30 minutes for redetermination applications. Through this matching operation, SSA eliminated the need for manual development (and thus the associated time) of these applications; FOs avoided manual verification of 635,567 initial applications and 13,649 redetermination applications for a total cost-savings of approximately $22,829,063.

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)

OCSS and SSA published notice of the relevant SORs in the *Federal Register*. SSA collects and maintains information exchanged under this agreement in the Medicare

Database (MDB) file SOR, No. 60-0321, last fully published at 71 Fed. Reg. 42159 (July 25, 2006), amended at 72 Fed. Reg. 69723 (December 10, 2007), and at 83 Fed. Reg. 54969 (November 1, 2018). The MDB contains information related to Medicare Part A, Part B, Medicare Advantage Part C, and Medicare Part D. This SOR has a routine use permitting the disclosure needed to conduct this match.

OCSS will disclose match results to SSA from the following system of records: *OCSS National Directory of New Hires*, System No. 09-80-0381; *see* SORN published in full at 89 Fed. Reg. 25625 (April 11, 2024). The disclosure of NDNH records by OCSS to SSA constitutes a "routine use," as defined by the Privacy Act. 5 U.S.C. § 552a(b)(3). Routine use (9) published in the NDNH SORN authorizes the disclosure of NDNH records to SSA.

The SORNs may be updated during the effective period of this agreement as required by the Privacy Act.

B. Number of Records Involved

SSA's Title XVIII Eligible table within MDB contains approximately 128 million records. The SSA finder file will contain approximately 10,000 records from the MDB each day. Once a month, SSA has an increased volume of approximately 200,000 in one of the daily exchanges. Once a year, the volume will increase by approximately 1.9 million records in the finder file to support the Extra Help process.

The NDNH contains approximately 1.5 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 (codified at 42 U.S.C. § 653(j)(4)), NDNH information provided to SSA by OCSS will contain all the available data elements from the QW and UI files, if any, pertaining to the individuals whose records are contained in the SSA finder file.

C. Specified Data Elements Used in the Match

1. **SSA will provide OCSS the following data elements electronically in the Finder File:**

   - Client's Own Social Security Number (COSSN)
   - Name

2. **OCSS will provide electronically to SSA the following data elements from the NDNH 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
     (2) Employer identification number
     (3) Address(es)
   - Transmitter Agency Code
   - Transmitter State Code
   - State or Agency Name

3. OCSS will provide electronically to SSA the following data elements from the NDNH UI file:

- UI record identifier
- Processed date
- SSN
- Verification request code
- Name (first, middle, last)
- Address
- UI benefit amount
- Reporting period
- Transmitter Agency Code
- Transmitter State Code
- State or Agency Name

4. Data Elements SSA updates in the OCSS Financial Items(OCSSFITM) table, if there is a match:

- QW record identifier
- For employees:
  (1) Employee's SSN
  (2) Employee's wage amount
  (3) Reporting period
- For employers of individuals:

  (1) Employer identification number
  (2) Employer's name
- UI identifier:

  (1) Claimant SSN
  (2) UI benefit amount
  (3) Reporting period
  (4) Transmitter State Name

D. Frequency of Data Exchanges

Data exchanges will be conducted daily, as follows.

OCSS Data Exchange Responsibilities

1. OCSS will compare the SSA finder file against the QW and UI files maintained in the NDNH for the purposes set forth in this agreement.

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

SSA Data Exchange Responsibilities

1. On a daily basis, SSA will submit a finder file containing all COSSNs to OCSS. The COSSNs are stored on SSA's OCSS Data Exchange Request Queue (OCSSQUE) table contained within the MDB.

2. SSA will request NDNH information for the following processes:

   - Medicare Part D daily screening operation
   - Medicare Part D subsidy process
   - Annual subsidy redetermination process

3. SSA will use the information provided by the comparison to administer the Extra Help program efficiently as set forth in this agreement.

4. Where there is a match, SSA will update the records in the OCSSFITM table contained within the MDB with the data elements received from OCSS.

E. 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. Only non-significant changes may be made in a modification; any significant changes would require a new agreement. SSA will conduct batch matches for Extra Help applicants or recipients with the NDNH database daily and will be conducted only as needed according to the purposes stated in this agreement. See also Section XII. For the effective dates.

The projected start date of this agreement is May 27, 2025, and the projected expiration date is November 26, 2026 (18 months from the start date), or November 25, 2027, if the agreement is renewed for one year. Any renewal will be signed in advance by OCSS, SSA and the respective DIB Chairpersons between August 26, and November 25, 2026, and will include OCSS' and SSA's certification that the requirements stated in section XII have been met.

OCSS may commence comparisons and disclosures under this agreement upon completion of all of the following requirements and the requirements stated in IV.C., below:

- OCSS and SSA agency officials (including DIB officials) sign the agreement; and
- SSA submits the documentation required by OCSS to assess the security posture of the agency.

IV.   NOTICE PROCEDURES

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) & (ii).

SSA provides, or will provide, the following notices to individuals whose records are used in the matching program established under this agreement.

A. Notice to Applicants

SSA directly notifies individuals at the time of application for Extra Help benefits regarding the comparison of their records against those of other agencies to determine eligibility. SSA's notice consists of appropriate language printed either on its application forms or on a separate handout when necessary. Medicare Extra Help notices are mailed, typically by an SSA vendor.

B. Notice to Recipients

SSA directly notifies Extra Help recipients of the comparison of records against those of other agencies to verify their continued eligibility for Extra Help at least once during the life of the agreement, including any extension to the agreement.

C. Notice to the General Public

SSA will publish a notice describing SSA's matching activities in the *Federal Register* informing the general public of this specific matching program. Both SSA and OCSS have published notice of their relevant SORs in the *Federal Register*.

SSA will publish the required public notice of matching program in the *Federal Register* at least 30 days prior to conducting the matching program. The notice cannot be published until SSA has reported the matching program to OMB and Congress for advance review and OMB has completed its advance 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*, 81 Fed. Reg. 94424 (December 23, 2016), at pages 17-23.

SSA will also provide a copy of the notice of matching program to OCSS immediately upon publication in the *Federal Register*; SSA and HHS will post the agreement and the published matching notice on their Privacy Program internet sites as required by OMB Memorandum M-23-22, *Delivering a Digital-First Public Experience* (September 22, 2023).

V. VERIFICATION PROCEDURES AND OPPORTUNITY TO CONTEST FINDINGS

The Privacy Act at 5 U.S.C § 552a(o)(1)(E) requires that each matching agreement specify procedures for verifying information produced in the matching program as required by 5 U.S.C. § 552a(p). The verification requirements outlined in 5 U.S.C. § 552a(p) include a requirement to give the affected individual notice of, and an opportunity to contest, unfavorable information before the agency uses the information to take an adverse action against the individual.

SSA recognizes that a match 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 MBD SOR. SSA will compare the identity of 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 in the NDNH.

If the individual is unable to confirm the information, SSA will contact the employer shown by the NDNH QW information to confirm the information shown by the comparison results, and the appropriate source agency to confirm the UI payment information. 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

Before making an unfavorable decision on an Extra Help application or redetermination based on the comparison results received from the match, SSA will provide a written, Pre-Decisional Notice (for initial Extra Help applications) or Notice of Planned Action (for redeterminations) to each individual for whom SSA decides such adverse action is necessary with the following information:

1. SSA received information that will have an adverse effect on the individual's eligibility for Extra Help;
2. Explain the effective date of any adjustment;
3. The individual has 10 days to contest any adverse decision and submit evidence, if required, to support a decision that a full or partial subsidy should be awarded, before SSA takes any adverse action because of the comparison information.
    20 CFR 418.3501, 418.3505, and 418.3510, and
4. Unless the individual contests the proposed adverse action in the required 10-day time period, SSA will conclude that the information provided by OCSS is correct and will make the necessary determination of eligibility for Extra Help.

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).

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

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

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

1. SSA will store and retain the electronic comparison files of the batch match only for the

time required to support the matching program and will then destroy the records. NDNH information will not be duplicated or disseminated within or outside SSA, without the written permission of 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 retain identifiable records received from the NDNH only for the period of time required for any processing related to the matching program and will then destroy the records.

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 the Privacy Act at 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 agreement, including the security addendum, specifies procedures for ensuring the security of such records.

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 Federal Information Security Management Act of 2002, as amended by the Federal Information Security and Modernization Act of 2014 (FISMA), 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 National Institute of Science and Technology (NIST) standards. These laws, directives, and standards include requirements for safeguarding federal information systems and PII used in federal agency business processes, as well as related reporting requirements. Laws, regulations, NIST standards, and OMB directives relating to the subject of this agreement, including those published subsequent to the effective date of this agreement, must be implemented by both agencies.

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

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

A. Breach Reporting

If either SSA or OCSS experiences an incident involving the suspected or confirmed breach (i.e., loss) of PII provided by SSA or OCSS under the terms of this agreement, they will follow the incident 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 breach will notify the other agency's point of contact named in this agreement. If OCSS is unable to speak with the SSA Office of Privacy and Disclosure Breach Contact within one hour or if for some other reason notifying the SSA Office of Privacy and Disclosure Breach Contact is not practicable (e.g., it is outside of the normal business hours), OCSS will call SSA's National Network Service Center at 1-877-697-4889. If SSA is unable to speak with OCSS' Systems Security Contact within one hour, SSA will contact OCSS' Director of Operations at Perimeter East Building, Baltimore, MD at 877-697-4889.

B. Breach Notification

SSA and OCSS will follow PII breach notification policies and related procedures issued

by OMB and other applicable legal, regulatory, and administrative authorities. If the agency that experienced the breach determines that the risk of harm requires notification to affected individuals or other remedies, that agency will carry out these remedies without cost to the other agency.

C. Administrative Safeguards

SSA and 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 their 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 an unauthorized person 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 the authorized analyst to perform their official duties.

F. Application of Policy and Procedures

SSA and OCSS have adopted policies and procedures to ensure that their respective agencies use the information contained in their respective records or obtained from each other solely as provided in this agreement. 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, 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 records to the source agency or destruction of records used in such program. 5 U.S.C. § 552(o)(1)(I).

A. Limitations of the Use of Information by OCSS

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

1. SSA finder files, and the information contained therein, will not be duplicated or disseminated within or outside OCSS without the written approval of SSA, except as necessary within OCSS for backup of 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 and are handled as provided in sections VI and VII, once the matching activity authorized under this agreement is complete.

2. SSA finder files and any other information provided by SSA will be used and accessed by OCSS only for the purposes specified in this agreement.

3. SSA finder files are not used by OCSS to extract information concerning the individuals therein for any purpose not specified in this agreement.

B. Limitations on the Use of Information by SSA

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

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

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

3. NDNH information will not be duplicated, redisclosed, or disseminated within or outside SSA, without the written permission of OCSS, except as necessary within SSA for backup of ongoing operations of the matching program and 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.

4. Information provided by OCSS remains the property of OCSS and will be handled as provided in sections VI and VII once the matching activity authorized under this agreement is complete.

C. Penalties

Subsection 453(l)(1) of the Act requires that NDNH information and the results of comparisons using NDNH information shall not be used or disclosed except as expressly provided in section 453, subject to section 6103 of the Internal Revenue Code of 1986. 42 U.S.C. § 653(l)(1). Subsection 453(l)(2) provides that an administrative penalty (up to and including dismissal from employment), and a fine of $1,000 shall be imposed for each act of unauthorized access to, disclosure of, or use of, information in the NDNH by any officer or employee of the United States, or any other person, who knowingly and willfully violates the requirement. 42 U.S.C. § 653(l)(2). The penalty is subject to inflation adjustment as authorized by the Federal Civil Penalties Inflation Adjustment Improvement Act of 2015 (Section 701 of Pub. L. No. 114-74).
See 45 CFR 303.21(f) and 45 CFR 102.3.

IX. RECORDS ACCURACY ASSESSMENTS

The information contained in the NDNH is reported to OCSS by state and federal agencies and instrumentalities. OCSS verifies the accuracy of name and SSN combinations maintained in the NDNH 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 has a corresponding name and SSN within SSA's Enumeration System.

The SSA Enumeration System used for SSN matching is 100 percent accurate based on SSA's Office of Analytics, Review, and Oversight. All employee names and SSN combinations contained in the new hire and the UI files against which finder files are compared have been verified against SSA's Enumeration System. For QW, only 77 percent of the incoming data has a verified name and SSN combination, since some states and employers do not capture enough name information in their records to complete this process. However, information comparisons may be conducted and reliable results obtained.

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 the OCSS Reimbursable Agreement (RA) and FS Forms 7600A and 7600B. Moreover, 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:

- an RA, prepared by OCSS
- and FS Forms 7600A and 7600B prepared by SSA

All documents are signed by both OCSS and SSA. The RA and FS Forms 7600A and 7600B will be entered into each fiscal year and will address costs and reimbursement terms. SSA may incur obligations only on a fiscal year basis. SSA's ability to perform work for fiscal years beyond FY 2024 is subject to the availability of funds.

OCSS will collect funds from SSA by means of the Intra-governmental Payment and Collection (IPAC) system through Treasury's G-Invoicing system which will generate an 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

The Privacy Act provides that a copy of each matching agreement shall be transmitted to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Accountability 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).

The Privacy Act also provides that no agreement shall be effective until 30 days after the date on which a copy of the agreement is transmitted to such congressional committees. 5 U.S.C. § 552a(o)(2)(B). *See also*, notice and reporting requirements in
5 U.S.C. § 552a(e)(12) and 5 U.S.C. § 552a(r). OMB Circular A-108 at pages 18 and 20 requires that a matching notice be published in the *Federal Register* for at least 30 days before conducting matching under the agreement and that the notice cannot be published until OMB has completed its advance review of the agreement and the notice.

This agreement will be effective, and the comparison and disclosure of information under this agreement may commence, when the agencies comply with the Privacy Act notice and reporting requirements. Where applicable, agencies may agree upon a later effective date, for example to coincide with the expiration of a renewal of a previous matching program between the agencies. SSA and OCSS intend that the effective date of this agreement will be May 27, 2025, the day after the expiration date of the one- year renewal agreement, HHS No. 2501.

The effective date of this agreement will be May 27, 2025, provided that SSA 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, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,* (December 23, 2016) and that, upon completion of OMB's advance review, SSA published notice of the matching program in the *Federal Register* for at least 30 days in accordance with 5 U.S.C. § 552a(e)(12) and OMB Circular A-108.

B. Duration of the Agreement

The Privacy Act requires that a matching agreement will remain in effect only for such period, not to exceed 18 months, as the DIB of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct of the matching program. 5 U.S.C. § 552a(o)(2)(C). This agreement will remain in effect for a period of 18 months, subject to renewal by the DIBs of both agencies for a period of up to one year. The renewal may occur if OCSS and SSA can, and do, certify in writing to their DIBs that: (1) the matching program will be conducted without change, and (2) OCSS and SSA have conducted the matching program in compliance with the original agreement.

Both SSA and OCSS will sign FS Forms 7600A and 7600B, and a RA prior to the initiation of any services of this agreement and for each fiscal year in which this agreement is in effect.

C. Modification of the Agreement

This agreement may be modified at any time by a written modification, signed by both parties and approved by the HHS DIB and SSA DIB, provided that the changes are not significant. A significant change requires a new agreement.

D. Termination of the Agreement

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

- SSA has not met its requirement to reimburse OCSS under 42 U.S.C. §

653(k) as agreed upon in section XI of this agreement and the fiscal agreements of both SSA and OCSS;

- 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 OMB IT Dashboard, the Annual Report to Congress, and the Exhibit 300. OCSS is required to provide performance measures demonstrating how the FPLS supports OCSS' strategic mission, goals, 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 to OCSS a written description of the performance outputs and outcomes attributable to its use of NDNH information for the purposes set forth in this agreement.

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

The performance reports may also assist SSA in the development of a cost-benefit analysis of the matching program required for any subsequent matching agreements in accordance with 5 U.S.C. § 552a.

XIV. DISPUTE RESOLUTION

Disputes related to this Agreement must 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:
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
Telephone: (202) 260-4712
Email: Venkata.Kondapolu@acf.hhs.gov
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) 401-5568
Email: Angela.Kasey-Henry@acf.hhs.gov

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

B. SSAcontactsare: ProgramPolicy
Issues
Lindsay Noonan, Team Leader
DeathProcessing&MedicareTeam
Office of Earnings
Enumeration & Medicare Policy
Office of IncomeSecurity Programs
D-21 Robert M. Ball Building
6401 Security Boulevard
Baltimore,MD 21235-6401
Telephone: (410) 965-9041
Lindsay.Noonan@ssa.gov

ComputerSystems Issues
ColleenCarpenter, DivisionDirector
Division of Title 2
Computations, Eligibility and Medicare
DCS/OfficeofBenefitsInformationSystems
4313 Robert M. Ball Building
Baltimore,MD 21235-6401
Telephone:(410) 965-5178
Email: Colleen.Carpenter@ssa.gov

Office of Privacy and Disclosure Breach
Contact Andrea Huseth, Division Director
Office of Privacy and Disclosure
Office of the General Counsel
6401 Security Boulevard
Baltimore,MD 21235-6401
Telephone: (410) 965-6868
Email:Andrea.Huseth@ssa.gov

Matching Agreement Issues
SoniaRobinson,GovernmentInformationSpecialist
Office of Privacy and Disclosure
OfficeoftheGeneral Counsel
6401 Security Boulevard
Baltimore,MD 21235-6401
Telephone:(410) 966-4115
Email: Sonia.V.Robinson@ssa.gov

DataExchange Issues
FernParson-Hill,HHS Data Exchange Liaison
OfficeofDataExchangeandInternationalAgreements
Officeof DataExchange, PolicyPublications, andInternationalNegotiations
Office of Retirement and Disability Policy
4-B-7-C Annex Building
6401Security Boulevard
Baltimore, MD 21235
Telephone: (410)   966-3697
Email:Fern.Parson-Hill@ssa.gov

Stephanie Meilinger, Data Exchange Liaison
Officeof DataExchangeandInternationalAgreements
Officeof DataExchange, PolicyPublications, andInternationalNegotiations
Office of Retirement and Disability Policy
SocialSecurityAdministration
6401 Security Boulevard
Baltimore,MD 21235
Telephone:(410) 966-0476
Email: Stephanie.Meilinger@ssa.gov

Information Security Issues
Robert Muffoletto, Division Director
Division of Compliance and Assessments
Office of Information Security
Social Security Administration
Suite 3383 Perimeter East Building
6201 Security Boulevard
Baltimore, MD 21235-6401
Telephone: (410) 966-5248
Email: Robert.Muffoletto@ssa.gov

XVI.   INTEGRATION CLAUSE

This agreement, the Security Addendum, the appendices, FS Forms 7600A and 7600B, and the OCSS reimbursement agreement prepared and authorized at the start of each fiscal year throughout the life of the agreement constitute the entire agreement of the parties with respect to its subject matter and supersede all other data exchange agreements between the parties for the purposes described herein. The 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, including any conflicting terms in any Interconnection Security Agreement (ISA) entered into in accordance with NIST SP 800-47 governing the interconnections between information technology systems that will be utilized for the transfer of information under this agreement. This agreement does not supersede federal law or HHS and OMB directives.

XVII. APPROVALS

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

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

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

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

Linda A. Boyer -S Date: 2025.02.10 07:20:09 -05'00' Digitally signed by Linda A. Boyer -S	
Linda Boyer Deputy Commissioner Office of Child Support Services	**Date**

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

Andrew K. Gradison	
Andrew Gradison Acting Assistant Secretary Administration of Children and Families	**Date**

C. Social Security Administration

Michelle Christ Digitally signed by Michelle Christ Date: 2025.01.17 13:51:20 -05'00'	
Michelle L. Christ Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	**Date**

D. Data Integrity Boards

The respective Data Integrity Boards having reviewed this agreement and finding that it complies with applicable statutory and regulatory guidelines signify their respective approval by the signature of the officials appearing below.

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

U.S Department of Health and Human Services

Jennifer Wendel for Scott Rowell	
Scott W. Rowell Acting Chairperson	**Date** 3/27/2025

Social Security Administration

Matthew Ramsey Digitally signed by Matthew Ramsey Date: 2025.02.26 10:14:19 -05'00'	
Matthew D. Ramsey Chair SSA Data Integrity Board	**Date**

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

Verification of Eligibility for Extra Help (Low Income Subsidy) under the
Medicare Part D Prescription Drug Coverage Program
SSA # 1306/HHS # 2501

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 SSA 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 finder files and response 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 will 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, and other machine-readable information, the information systems of OCSS and SSA, and SSA authorized entities specified in the agreement, which are hereinafter referred to as "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 administrative, physical, and technical safeguarding requirements with which OCSS and SSA must comply and continuously monitor. SSA must also comply with three additional requirements: Breach Reporting and Notification Responsibility; Security Authorization; and Audit Requirements.

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

1. SSA must restrict access to, and disclosure of, NDNH information to authorized personnel who need NDNH information to perform their official duties in connection with the authorized purposes specified in this agreement. OCSS restricts access to, and disclosure of, the agency finder files to authorized personnel who need them to perform their official duties as authorized in this agreement.
    Policy/Requirements Traceability: 5 U.S.C. § 552a(b)(1). NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, AC-3, AC-6

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

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

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

3. SSA must advise all authorized personnel who will access NDNH information of the confidentiality of the 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(1)(2) of the Act. 42 U.S.C. § 653(1)(2).

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

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

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

   OCSS delivers security and privacy awareness training to personnel. The training describes each user's responsibility for proper use and protection of other agencies' finder 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 finder files and at least annually thereafter. The training covers the other federal laws governing use and misuse of protected information.

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

5. SSA personnel with authorized access to NDNH information must sign non-disclosure agreements, rules of behavior, or equivalent documents before system access, annually, and if changes in assignment occur. The non-disclosure agreement, rules of behavior, or equivalent documents will outline the authorized purposes for which 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 finder 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 finder files. The records will contain a copy of each individual's signed non-disclosure agreement, rules of behavior, or equivalent document, and proof of the individual's participation in security and privacy awareness training.

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

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

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

    OCSS does not permit personnel to access the agency finder 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 the SSA standards. All remote connections must be through a Network Access Control (NAC) solution; all data in transit between the remote location and SSA must be encrypted using FIPS 140-3 encryption standards. Personally owned mobile devices must not be authorized. See numbers 8 and number 19 of this section for additional information.

    OCSS does not permit personnel to access the agency finder 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 ensures 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 agency finder 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. Health and Human Services officials, as required.

    Policy/Requirements Traceability: NIST SP 800-53 Rev. 5, CA-7(1); 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 finder files.

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

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

    OCSS maintains a system security plan that describes the security requirements for the information system housing the agency finder 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 finder 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 finder files.

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

15. SSA must limit and control logical and physical access to NDNH information to only those personnel authorized for such access based on their official duties and identified in the records maintained by SSA pursuant to number 6 and number 27 of this section. SSA must prevent personnel from browsing case files not assigned to them by using technical controls or other compensating controls.
    OCSS limits and controls logical and physical access to the agency finder files to only those personnel authorized for such access based on their official duties. OCSS prevents browsing using technical controls that limit and monitor access to the agency finder files.
    Policy/Requirements Traceability: 5 U.S.C. § 552a; NIST SP 800-53 Rev. 5, AC-2, AC-3

16. SSA must transmit and store all NDNH information provided pursuant to this agreement in a manner that safeguards the information and prohibits unauthorized access. All electronic SSA transmissions of information to SSA and entities specified in the agreement shall be encrypted using a FIPS 140-3 compliant product. SSA and OCSS exchange data via a mutually approved and secured data transfer method which 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, 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 number 8 and number 18 of this section for additional information.
    OCSS does not copy the agency finder 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 finder 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 will control remote access through a limited number of managed access control points.
    OCSS prohibits remote access to the agency finder files except via a secure and encrypted (FIPS 140-3 compliant) transmission link and using two-factor authentication as required by OMB M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*
    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

regularlyreviewed 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/RequirementsTraceability: NIST SP 800-53 Rev. 5, AU-2, AU-3, AU-6(1)(3), AU-8, AU-9(4), AU-11

21. SSA must log each computer-readable data extract (secondary store or files with duplicate NDNH information) from any databases holding NDNH information and verify that each extract has been erased within 90 days after completing required use. If SSA requires the extract for longer than 90 days to accomplish a purpose authorized pursuant to this agreement, SSA 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.

    OCSSdoes not extract information from the agency finder files.

    Policy/RequirementsTraceability: OMBM-17-12; NIST SP 800-53 Rev. 5, MP-4, MP-6, SI-12

22. SSA must use 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 sections 8, 9, and 18 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/RequirementsTraceability: OMBM-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.

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

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

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

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

25. SSA must implement a Network Access Control (also known as Network Admission Control (NAC) solution in conjunction with a Virtual Private Network (VPN) option to enforce security policy compliance on all SSA and non-SSA remote devices that attempt to gain access to, or use, NDNH information. SSA must use a NAC solution to authenticate, authorize, evaluate, and remediate remote wired and wireless users before they can access the network. The implemented NAC solution must evaluate whether remote machines are compliant with security policies through host(s)' integrity tests against predefined templates, such as patch level, service packs, antivirus, and personal firewall status, as well as custom-created checks tailored for the SSA enterprise environment. SSA must disable functionality that allows automatic execution of 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 finder 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 the NDNH information complies with the security requirements established in this security addendum. The "data processing facility" includes the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information, and the information systems of 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 pursuant to this agreement in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

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

Policy/Requirements Traceability: NIST SP 800-53 Rev. 5, PE-2, PE-3

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

OCSS maintains a list of personnel authorized to access facilities and systems processing the agency finder files. OCSS controls access to facilities and systems wherever the agency finder 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 shall not transport NDNH information off SSA and permitted entities premises. When no longer needed, in accordance with the retention and disposition requirements in the agreement, SSA must destroy these printed reports by burning or shredding.

OCSS does not generate printed reports containing the agency finder files information.

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. CLOUDSOLUTION(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 140-3 validated modules. Adequate logging controls must be in place to determine key changes and access.

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

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

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

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

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

9. The data stored by the cloud service provider must 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 and services 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 OCSS' security team as designated in this security addendum. Incident reporting contact information is in this security addendum (*See* section VIII). SSA is responsible for all reporting and notification activities, including but not limited to: investigating the incident; communicating with CISA; notifying individuals whose information is breached; notifying any third parties including the media; notifying any other public and private sector agencies involved; responding to inquiries about the breach; responding to Congressional inquiries; resolving all issues surrounding the information breach; performing any follow-up activities; correcting the vulnerability that allowed the breach; and any other activity as required by OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and other federal law and guidance.

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 within one hour, of if for some reason notifying the SSA security contact is not practicable (e.g., it is outside of the normal business hours), OCSS will call SSA's National Network Service Center toll free at 1-877-697-4889. 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-

VI.   SECURITY AUTHORIZATION

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

1.   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 the NDNH information on SSA premises.

The SSA ATO was signed on February 25, 2022. OCSS considers this evidence that the SSA environment complies with the security requirements in this security addendum.

The effective period for an ATO is three years. SSA must provide a signed ATA 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.

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

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 commensurate with those of a federal system categorized as "moderate" according to FIPS 199. See also: OMB M-24-04, Fiscal Year 2024 Guidance on Federal Information Security and Privacy, December 4, 2023.

AUDIT REQUIREMENTS

Section 453(m)(2) requires that the Secretary of Health and Human Services establish and implement safeguards to restrict access to confidential information to authorized persons, and for authorized purposes. 42 U.S.C. § 653(m)(2). OMB's guidance provides that since information security remains the responsibility of the originating agency, procedures should be agreed to, in advance, that provide for 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, December 20, 2010. See also, section 453(l)(2) of the Social Security Act (42 U.S.C. § 653(l)(2) and 5 U.S.C. § 552a(e)(10)).

Policy/Requirements Traceability: OMB M-24-04, Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements, December 4, 2023; OMB Circular No. A-130, Appendix I

VII. 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 ChildSupport Services
Administration for Children and Families
Mary E. Switzer Building
330 C Street, SW
Washington,DC 20201
Phone:(202) 260-4712
Email: 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 Social Security Administration contact is:

Robert Muffoletto, Director
Division of Compliance and Assessments
Office of Information Security
Office of Systems
Social Security Administration
6201 Security Boulevard, Suite 3383
Perimeter East Building
Baltimore, MD 21235-6401
Phone:(410) 966-5248
Email: Robert.Muffoletto@ssa.gov

VIII.   APPROVALS

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

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

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

Venkata Kondapolu -S Digitally signed by Venkata Kondapolu -S Date: 2025.02.05 12:09:49 -05'00'	
Venkata Kondapolu Director Division of Federal Systems Office of Child Support Services	**Date**
Linda A. Boyer -S Date: 2025.02.10 07:20:54 -05'00' Digitally signed by Linda A. Boyer -S	
Linda Boyer Deputy Commissioner Office of Child Support Services	**Date**

B.   Social Security Administration

Robert Muffoletto Date:2025.01.24 10:14: Digitally signed by Rober	tMuffoletto 1 -05'00'
Robert Muffoletto Division Director Division of Compliance and Assessments Office of Information Security	**Date**
Michelle Christ Digitally signed by Michelle Christ Date: 2025.01.17 14:23:04 -05'00'	
Michelle L. Christ Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	**Date**

APPENDIX A

Background: Current Agreements Between OCSS
and
SSA "Extra Help" Prescription Drug Subsidy Match

The data exchange 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). OCSS and SSA have entered into matching agreements and renewals for this matching program since April 2005, the latest of which expires November 26, 2026.

All authorized purposes for which the NDNH information is disclosed to SSA and all authorized persons and entities to be disclosed NDNH information are combined herein.

Prior Computer Matching agreements between the parties related to the Verification of Eligibility for Extra Help (Low Income Subsidy) under the Medicare Part D Prescription Drug Coverage Program are:

- Computer Matching Agreement between SSA and OCSS, Administration for Children and Families, Department of Health and Human Services (ACF, HHS) (SSA Match # 1306/HHS # 1705), "Verification of Eligibility for Prescription Drug Subsidy Match," effective November 27, 2017 through May 26, 2019; Recertification of Computer Matching Agreement effective May 27, 2019 through May 26, 2020.

- Computer Matching Agreement between SSA and OCSS, ACF, HHS (SSA Match # 1306/HHS # 1407), "Verification of Eligibility for Prescription Drug Subsidy Match," effective April 1, 2015, through October 31, 2016; Recertification of Computer Matching Agreement effective November 1, 2016, through October 31, 2017.

- Computer Matching Agreement between SSA and OCSS, ACF, HHS (SSA Match # 1306/HHS # 1203), "Verification of Eligibility for Prescription Drug Subsidy Match," effective October 1, 2012, through March 31, 2014; Recertification of Computer Matching Agreement effective April 1, 2014, through March 31, 2015.

- Computer Matching Agreement between SSA and OCSS, ACF, HHS (SSA Match # 1306/HHS # 0903), "Verification of Eligibility for Prescription Drug Subsidy Match," effective March 20, 2010, through September 30, 2011; Recertification of Computer Matching Agreement effective October 1, 2011, through September 30, 2012.

- Computer Matching Agreement between SSA and OCSS, ACF, HHS (SSA Match # 1306/HHS # 0702), "Verification of Eligibility for Prescription Drug Subsidy Match," effective September 20, 2007, through September 19, 2009; Recertification of Computer Matching Agreement effective March 20, 2009, through September March 19, 2010.

- Computer Matching Agreement between SSA and OCSS, ACF, HHS (SSA Match # 1306/HHS # 0409), "Verification of Eligibility for Prescription Drug Subsidy Match," effective April 1, 2005, through September 30, 2006; Recertification of Computer Matching Agreement effective October 1, 2006, through September 30, 2007.

APPENDIX B
DEFINITIONS

FOR
THE COMPUTER MATCHING AGREEMENT

BETWEEN

OCSS AND SSA

Verification of Eligibility for Extra Help (Low Income Subsidy)
under the Medicare Part D Prescription Drug Coverage Program

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

"Disclose" and **"disclosure"** mean the release of information by SSA or OCSS, with or without the consent of the individual(s) to whom the information pertains.

"Extra Help" means the low-income subsidy assistance Medicare beneficiaries receive under the Medicare prescription drug program if they have limited income and resources. SSA certifies to HHS that an individual can receive Extra Help to pay for Medicare prescription drug plan costs such as monthly premiums, annual deductibles, and prescription co-payments.

"Low-income subsidy eligible individual" means a Medicare Part D eligible individual who lives in one of the 50 states, the District of Columbia, or territories and enrolls or seeks enrollment in a prescription drug plan or Medicare Advantage Plan, and who meets all the requirements under section 1860D-14 of the Act and applies for Extra Help.

"Part D" means the voluntary Medicare prescription drug benefit program for all individuals eligible for Medicare Part A, Part B, or both, under which the individuals pay a monthly premium for coverage, deductibles, and copayments to help purchase covered prescription drugs.

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

"Recipient agency" means any agency, or contractor thereof, receiving records contained in a SOR from a source agency for use in a matching program. 5 U.S.C. § 552a(a)(9).

"Source agency" means any agency disclosing records contained in a SOR for use in a matching program, or any state or local government, or agency thereof, disclosing records for use in a matching program. 5 U.S.C. § 552a(a)(11).

APPENDIX C
CostBenefit Analysis for

MedicarePartDMatchingOperationbetween

Social SecurityAdministration(SSA)andOfficeofChildSupportServices(OCSS)(Match#1306)

Objective of the matching operation

The purpose of the matching operation is to verify attestations regarding income and resources made by claimants for Medicare Part D prescription drug subsidy assistance under the Medicare Modernization Act (MMA) of 2003.

Background

The MMA provides deductible and co-payment subsidies for certain low-income individuals to receive Medicare Part D premiums. The MMA requires that we take applications and determine eligibility for this subsidy program, since lawmakers designed the program to assist individuals with limited financial means in paying for the prescription drug coverage. We automatically deem eligible individuals who have Medicare and receive Supplemental Security Income (SSI) or Medicaid, or who participate in the Medicare Savings Program. SSA determines eligibility for full or partial subsidy by comparing income and resource information provided by applicants with income and resource data available in our systems, as well as data obtained through matching agreements with other agencies.

Methodology

The Office of Data Exchange and International Agreements (ODXIA) reviewed initial and redeterminationsubsidy application data for beneficiaries who have matching income or resource data from SSA and OCSS.

Specifically, ODXIA identified the number of applications excluded from the verification process to determine the cost-savings for avoiding verification of income and resource application data for beneficiaries, who applied for and are receiving Medicare Part D subsidies. We identified and eliminated applications denied during the screening out process from the counts even though they still go through the matching process. We concentrated on capturing data for cases awarded or denied due to the computer matching process, without manual intervention.

COSTS

Thetotal FY 2023 personnel and computer costs for this matching operation is **$880,421.**

KeyElement1:PersonnelCosts
For Agencies –

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

  Field Office (FO) Development

  This CBA focuses on the cost-savings gained by eliminating FO personnel involvement in the manual verification of Medicare Part D subsidy application income and resource allegations. Therefore, there are no personnel costs attributable to this matching operation.

- JusticeAgency – (N/A)

For Clients – N/A
ForThird Parties – N/A
Forthe General Public – N/A

Key Element 2: Agencies' Computer Costs For Agencies -

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

For FY 2023, the Office of Systems reports a computer cost of $26,021.

Justice Agencies – N/A

Interagency Agreement Cost
For FY 2023, the total cost of the IAA for this matching operation is **$854,400**.

BENEFITS

The benefit of conducting this matching operation is the increased accuracy of our subsidy determinations, and the cost-savings gained by reducing the need for manual verifications by FO of all income and resource allegations on Medicare Part D subsidy initial and redetermination applications.

For FY 2023, the total cost savings benefits realized from this matching operation total is approximately **$22,829,063.**

Key Element 3:

Avoidance of Future Improper

Payments
To Agencies –

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

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

Conclusion

Section 1144 of the Act requires SSA to conduct outreach efforts for the Medicare Savings Programs and subsidized Medicare prescription drug coverage. However, SSA does benefit from administrative savings by avoiding the cost of manual development of income and resources reported on initial and redetermination applications. We estimate that the benefit-to-cost ratio for this matching operation is **25.9:1.** Therefore, we recommend the continuation of this matching operation.

CostBenefit Analysis for
MedicarePartD Matching Operation between
SocialSecurityAdministration (SSA) and Office of Child Support Services (OCSS) (Match #1306)

Cost Summary

Interagency Agreement Cost	$854,400
Systems Costs	$26,021
Total Costs	**$880,421**

Benefits Summary (Verification Costs Avoided due to Match)

Number of Initial Application Verifications Avoided	635,567
Unit Cost for Initial Application Verification [1]	$35.43
Total Initial Application Verification Costs Avoided due to Match	**$22,518,139**
Number of Redetermination Verifications Avoided	13,649
Unit Cost for Redetermination Verification [1]	$22.78
Total Redetermination Verification Costs Avoided due to Match	**$310,924**
Total Number of Verifications Avoided	649,216
Total Benefit	**$22,829,063**
Benefit-to-Cost Ratio	**25.9**

---

[1] Unit costs are calculated using unit times provided by the Office of Public Service and Operations Support, and FO cost per workyear and overhead rates provided by the Office of Finance.

Appendix D
BusinessNeedsAssessmentChart
forthePrescriptionDrugMatching Agreementbetween OCSSandSSA

SSA Application	Match Method	Function	Elements Provided by SSAtoConduct Match	Elements ProvidedbyOCSSto Conduct Match	SSAUser	Elements SSA will updateinthematch	OCSS Databases	Authority
Medicare Data Base (MDB) Office of Child Support Services Data Exchange Request Queue (OCSSQUE) Table	Batch	To determine eligibility of applicantsforExtra Help (low-income subsidyassistance) undertheMedicare Prescription Drug, Improvement, and Modernization Act of 2003	Client's Own SocialSecurity Number (COSS)(SSN), and Name	From the Quarterly Wage File: quarterly wage record identifier; for employees: name, SSN, verification request code, processed date, non-verifiable indicator, wage amount, and reporting period; for employers of individuals: name, employer identification number (EIN), and addresses; transmitter agency code, transmitter state code, state or agency name. From the UI File: UI record identifier, processed date, SSN, verification request code, name, address, UI benefit amount, reporting period, transmitter agency code, transmitter state code, and state or agency name.	personnel are responsible for determining eligibility for Extra Help.	Quarterlywagerecord identifier, name, SSN, processed date, address(es), wage amount,quarterlywage reporting period. Employers name, transmitted agency codeemployeraddress (es). UI record identifier, processed date, UI benefit amount, and reporting period.	National Directoryof New Hires (NDNH) - Quarterly WageFileand UI File	42 U.S.C. § 653(j)(4), 42 U.S.C. § 1383(f), and 42 U.S.C. §1395w-114(a)(3)(B)