COMPUTER MATCHING AGREEMENT

BETWEEN

SOCIAL SECURITY ADMINISTRATION

AND

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

"Verification of Eligibility for Extra Help (Low Income Subsidy) under the
Medicare Part D Prescription Drug Coverage Program"
SSA Match # 1306/HHS Match # 2003

I.   PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

A. Purpose of the Matching Agreement

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

This agreement 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.

The Privacy Act provides that no record contained in a system of record (SOR) may be disclosed for use in a computer matching program, except pursuant to a written agreement containing specified provisions. 5 U.S.C. § 552a(o). SSA and OCSE are executing this agreement to comply with the Privacy Act and the regulations and guidance promulgated thereunder. OCSE and SSA have been parties to matching agreements and recertifications 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 OCSE is the Division of Federal Systems.

This agreement is applicable to personnel, facilities, and information systems of SSA and OCSE involved in the processing and storage of NDNH information. Personnel are defined as employees, contractors, or agents of OCSE 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 OCSE shall provide the Commissioner of SSA with all information in the NDNH. 42 U.S.C. § 653(j)(4). SSA has authority to use data to determine entitlement to and eligibility for programs it administers pursuant to sections 453(j)(4), 1631(e)(1)(B) and(f), and 1860D-14(a)(3) of the Act. 42 U.S.C. §§ 653(j)(4), 1383(e)(1)(B) and (f), and 1395w-114(a)(3). Disclosures under this agreement shall be made in accordance with 5 U.S.C. § 552a(b)(3), and in compliance with the matching procedures in 5 U.S.C. § 552a(o), (p), and (r).

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

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

B. Other Supporting Justifications

The matching program reduces the enrollment burden on Medicare beneficiaries and expedites the enrollment process. Additionally, this matching program ensures a correct Extra Help program eligibility determination while reducing the level of effort SSA Field Offices (FO) 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 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 17.6:1.

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 reduces overpayments. 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.

C. Specific Estimate of Any Savings

The benefit to SSA 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 by FOs of all income and resource allocations on Medicare Part D subsidy initial and redetermination applications.

For fiscal year (FY) 2018, 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 495,884 initial applications and 16,843 redetermination applications for a total cost-savings of approximately $15,909,954.

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

OCSE and SSA published notice of the relevant system of records 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), and amended at 72 Fed. Reg. 69723 (December 10, 2007), and 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. The information in this SOR may be updated during the effective period of this agreement as required by the Privacy Act.

OCSE will match SSA information in the MDB against the QW and UI information furnished by state and federal agencies maintained in its SOR, "OCSE National Directory of New Hires" (NDNH), No. 09-80-0381, published in the *Federal Register* on April 2, 2015 at 80 Fed. Reg. 17906 and amended at 83 Fed. Reg. 6591 (February 14, 2018). The disclosure of NDNH information by OCSE to SSA constitutes a "routine use," as defined by the Privacy Act. 5 U.S.C. § 552a(b)(3). Routine use (9) of the SOR authorizes disclosure of NDNH information to SSA, 80 Fed. Reg. 17906, 17907 (April 2, 2015).

B. Number of Records Involved

SSA's Title XVIII Eligible (T18ELG) table within MDB contains approximately 90 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 represents the most recent 24 months of information. In accordance with section

453(j)(4) of the Act, NDNH information provided to SSA by OCSE will contain 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.   42 U.S.C. § 653(j)(4).

C. Specified Data Elements Used in the Match

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

   - COSSN (SSN)
   - Name

2. **OCSE 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. **OCSE 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 <u>in the OCSEFITM</u> 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
- Unemployment Insurance identifier:
  (1) Claimant SSN
  (2) Unemployment insurance benefit amount
  (3) Reporting period
  (4) Transmitter State Name

D. **Frequency of Data Exchanges**

OCSE Responsibilities

1. On a daily basis, OCSE 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. OCSE will send a response file to SSA containing the results of this comparison.

SSA Responsibilities

1. On a daily basis, SSA will submit a finder file containing all Clients' Own Social Security Numbers (COSSN) to OCSE. The COSSNs are stored on SSA's OCSE Data Exchange Request Queue (OCSEQUE) table contained within the MDB.

2. SSA requests 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 OCSE Financial Items (OCSEFITM) table contained within the MDB with the data elements received from OCSE.

5. SSA will publish the *Federal Register* notice and submit the letters to Congress and the Office of Management and Budget for this agreement.

E. Projected Start and Completion Dates

The starting and completion dates of the matching program are consistent with the effective and expiration dates of this agreement. The matching program will continue in effect until it expires unless terminated as stated in this agreement. SSA will conduct matches with the NDNH daily.

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 the Office of Management and Budget, to applicants for and recipients of financial assistance or payments under federal benefit programs, that any information provided by such applicants and recipients may be subject to verification through matching programs. 5 U.S.C. § 552a(o)(1)(D)(i) & (ii).

This requirement is best accomplished by direct notice pursuant to the Privacy Act on the application form, or on a separate form that can be retained by the individual. 5 U.S.C. § 552a(e)(3). SSA and OCSE provide the following additional notices, respectively, to persons whose records are disclosed from the SORs involved in the matching program established under this agreement.

A. Notice to the General Public

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

B. Notice to Applicants

SSA will notify 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.

C. Notice to Recipients

SSA will notify 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.

V. VERIFICATION PROCEDURES AND OPPORTUNITY TO CONTEST FINDINGS

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

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 SORs. 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 C.F.R. §§ 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 OCSE 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, OCSE and SSA shall destroy the records in accordance with the security addendum herein, including the erasure of all electronic records.

OCSE 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 OCSE.

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

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

2. SSA will 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.

3. This matching program generates some information that SSA must retain regarding some individuals to meet evidentiary requirements. SSA places printouts of the comparison results regarding specific individuals in the SSA claim folders of the involved individuals. SSA personnel dispose of the printouts in accordance with the appropriate National Archives and Records Administration federal records retention schedule. 44 U.S.C. § 3303a.

Neither SSA nor OCSE will create a separate file or SOR concerning individuals in the matching program, other than SSA records needed for integrity and audit purposes. Both SSA and OCSE will keep an accurate accounting of disclosures from an individual's records as required by the Privacy Act. 5 U.S.C. § 552a(c).

VII. SECURITY PROCEDURES

The Privacy Act requires that each matching agreement specify procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs. 5 U.S.C. § 552a(o)(1)(G).

SSA and OCSE will comply with the requirements of the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3541 et seq.; related Office of Management and Budget (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) directives. These laws, directives, and regulations include requirements for safeguarding federal information systems and personally identifiable information (PII) used in federal agency business processes, as well as related reporting requirements. Laws, regulations, NIST standards, and OMB directives relating to the subject of this agreement and published subsequent to the effective date 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 shall be taken and considered as a part of this agreement as if the provisions contained in the addendum were fully set out here.

A. Loss Reporting

If either SSA or OCSE experiences an incident involving a loss of PII provided by SSA or OCSE under the terms of this agreement, they will follow Office of Management and Budget loss reporting guidelines (OMB M-06-19 *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security into IT Investments*) (July 12, 2006). In the event of an incident involving the loss or potential loss of PII, the agency experiencing the event is responsible for following its established procedures, including notification to the proper organizations, such as the United States Computer Emergency Readiness Team (US-CERT). In addition, the agency experiencing the loss of PII will notify the other agency's Systems Security contact named in this agreement. SSA or OCSE, as appropriate, will also call SSA's National Network Service Center toll free at 877-697-4889. If SSA is unable to speak with OCSE's Systems Security Contact within one hour, SSA will contact OCSE's Director of Operations at PEB, Baltimore, MD 877-697-4889.

B. Breach Notification

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

C. Administrative Safeguards

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

D. Physical Safeguards

SSA and OCSE will store the data matched and any data created by the match in an area that is physically and technologically secure from access by unauthorized person at all times (e.g., door locks, card keys, biometric identifiers, etc.). Only authorized personnel will transport the data matched and any data created by the match. SSA and OCSE will establish appropriate safeguards for such data, as determined by a risk-based assessment for the circumstances involved.

E. Technical Safeguards

SSA and OCSE will process the data matched and any data created by the match under the immediate supervision and control of authorized personnel in a manner that will protect the confidentiality of the data, so that unauthorized 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 OCSE will strictly limit authorization to those electronic data areas necessary for the authorized analyst to perform his or her official duties.

F. Application of Policy and Procedures

SSA and OCSE will adopt policies and procedures to ensure that their respective agencies use the information contained in their respective records or obtained from each other solely as provided in this agreement. SSA and OCSE will comply with these guidelines and any subsequent revisions.

G. Security Assessment

NIST Special Publication 800-37, as revised, 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 800-37 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 OCSE

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

1. SSA finder files, and the information contained therein, will not be duplicated or disseminated within or outside OCSE without the written approval of SSA, except as necessary within OCSE 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 information provided by SSA will be used and accessed by OCSE only for the purposes specified in this agreement.

3. SSA finder files are not used by OCSE 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 OCSE:

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 OCSE, except as necessary within SSA for backup of ongoing operations of the matching program and for the purpose of disaster recovery. OCSE will not grant such authority unless the disclosure is required by law or is essential to the matching program.

4. Information provided by OCSE remains the property of OCSE 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 Penalty Inflation Adjustment Improvement Act of 2015 (Section 701 of Pub. L. No. 114-74).
See 45 C.F.R. § 303.21(f) and 42 C.F.R. § 102.3.

IX. RECORDS ACCURACY ASSESSMENTS

The information contained in the NDNH is reported to the source agency by state and federal agencies and instrumentalities. OCSE verifies the accuracy of name and SSN combinations maintained by OCSE against SSA's Master File of SSN Holders and SSN Applications (Enumeration System), in accordance with section 453(j)(1)(A) and (B) of the Act. 42 U.S.C. § 653(j)(1)(A) and (B). A record reported to the NDNH is considered "verified" if the name and SSN combination 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). OCSE and SSA agree that the Comptroller General may have access to such records for the authorized purpose of monitoring or verifying compliance with this agreement.

XI. REIMBURSEMENT/FUNDING

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

OCSE will collect funds from SSA through the Intra-Governmental Payment and Collection (IPAC) system. OCSE will bill SSA twice during the fiscal year in accordance with the amounts and terms outlined in the RA and SSA-429. SSA will remit payment no later than fifteen 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 Government Reform of the House of Representatives and be available upon request to the public in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals. 5 U.S.C. § 552a(r) and (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).

This agreement shall 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 OCSE intend that the effective date of this agreement shall be May 27, 2020, the day after the expiration date of the recertification agreement, HHS No. 1407.

The effective date of this agreement is May 27, 2020, 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 OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,* (December 23, 2016) and that SSA published notice of the matching program in the *Federal Register* in accordance with 5 U.S.C. § 552a(e)(12).

B. Duration of the Agreement

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

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

C. Modification of the Agreement

This agreement may be modified at any time by a written modification, which is signed by both parties and approved by the U.S. Department of Health and Human Services (HHS) DIB and SSA DIB.

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 does not meet its requirement to reimburse OCSE under 42 U.S.C. § 653(k) as agreed upon in section XI of this agreement and the fiscal agreements of both SSA and OCSE;

- OCSE has reason to believe that the verification and opportunity to contest requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met pursuant to 5 U.S.C. § 552a(q)(1);

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

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

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

XIII.   PERIODIC REPORTING OF PERFORMANCE OUTCOMES

OMB requires OCSE to periodically report measures of the performance of the Federal Parent Locator Service (FPLS), including the NDNH, through various federal management devices, such as the Office of Management and Budget IT Dashboard, the Annual Report to Congress, and the Exhibit 300. OCSE is required to provide performance measures demonstrating how the FPLS supports OCSE's strategic mission, goals, objectives, and cross-agency collaboration. OCSE also requests such performance reporting to ensure matching partners use NDNH information for the authorized purpose.

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

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

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

XIV. DISPUTE RESOLUTION

Disputes related to this agreement over financial or accounting shall be resolved in accordance with instructions provided in the Treasury Financial Manual (TFM) Volume I, Bulletin No. 2013-04, Attachment I, *Procedures for Intergovernmental Transactions (ITGs)*, section II.D or a superseding directive, available on the TFM website at http://tfm.fiscal.treasury.gov/v1.html#Part2.

XV. PERSONS TO CONTACT

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

Venkata Kondapolu, Acting Director
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
Mary E. Switzer Building
330 C Street, SW, 5th Floor
Washington, DC 20201
Phone: 202-260-4712
Fax: 202-401-5558
Email: venkata.kondapolu@acf.hhs.gov

Maureen Henriksen, OCSE Liaison with SSA for Data Exchange
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
Mary E. Switzer Building
330 C Street, 5th Floor
Washington, DC 20101
Phone: 202-205-3848
Fax: 202-401-5558
Email: Maureen.Henriksen@acf.hhs.gov

B. Social Security Administration contacts are:

Program Policy Issues
Monica Nolan, Team Leader, Medicare Team
Office of Earnings, Enumeration & Medicare Policy
Office of Income Security Programs
D-21 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 965-2075
Email: Monica.Nolan@ssa.gov

Computer Systems Issues
Melanie Burns, Director
OBIS, DCMECE
Office of Systems
Office of Software Engineering
4817 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 966-0444
Email: Melanie.Burns@ssa.gov

Matching Agreement Issues
Sonia Robinson, Government Information Specialist
Office of Privacy and Disclosure
Office of the General Counsel
6401 Security Boulevard, G-401 WHR
Baltimore, MD 21235-6401
Phone: (410) 966-4115
Fax: (410) 966-4304
Email: Sonia.V.Robinson@ssa.gov

Data Exchange Issues
Stephanie Brock, HHS Data Exchange Liaison
Office of Data Exchange Policy Publications and International Negotiations
Office of Retirement and Disability Policy
4-B-7-C Annex Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (667) 305-5699
Email: Stephanie.Brock@ssa.gov

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

XVI.   INTEGRATION CLAUSE

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

XVII.   APPROVALS

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 shall be binding or recognized, and hereby commit their respective organizations to the terms of this agreement.

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

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

/s/	
Scott M. Lekan Commissioner Office of Child Support Enforcement	**Date** 1/13/2020

B. Social Security Administration

/s/	
Mary Ann Zimmerman Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	**Date** 1/14/2020

C. **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.

/s/	
Scott W. Rowell Chairperson Data Integrity Board Department of Health and Human Services	**Date** 3/17/2020

/s/	
Matthew D. Ramsey Acting Chair SSA Data Integrity Board Social Security Administration	**Date** 1/29/2020

SECURITY ADDENDUM

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

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 # 2003

I.   PURPOSE AND EFFECT OF THIS SECURITY ADDENDUM

The purpose of this security addendum is to specify the security controls that the Office of Child Support Enforcement (OCSE) and the Social Security Administration (SSA) shall have in place to ensure the security of the records compared against records in the National Directory of New Hires (NDNH) and the results of the information comparison.

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

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

II.   APPLICABILITY OF THIS SECURITY ADDENDUM

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

III.   SECURITY AND PRIVACY SAFEGUARDING REQUIREMENTS

SSA shall comply with the *Office of Child Support Enforcement Division of Federal Systems*

Security Requirements for Federal Agencies Receiving Federal Parent Locator Service Data. SSA received this document on May 14, 2019. The safeguarding requirements in this security addendum are drawn from this document and are also based on the federal laws and requirements governing the protection of information referenced in section I of this security addendum.

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

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

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

   OCSE restricts access to and disclosure of the agency input 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 4, AC-3, & AC-6

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

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

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

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

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

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

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

   OCSE delivers security and privacy awareness training to personnel. The training describes each user's responsibility for proper use and protection of other agencies' input files, how to recognize and report potential indicators of insider threats, and the possible sanctions for misuse. All personnel receive security and privacy awareness training before accessing agency input files and, at least, annually thereafter. The training covers the other federal laws governing use and misuse of protected information.

   Policy/Requirements Traceability: 5 U.S.C. § 552a; 44 U.S.C. § 3551 et seq; OMB Circular A-130, *Managing Information as a Strategic Resource*; OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (November 23, 2016);* NIST SP 800-53 Rev 4, AT-2(2), AT-3

5. SSA personnel with authorized access to NDNH information shall sign non-disclosure agreements, rules of behavior, or equivalent documents before system access annually, and if changes in assignment occur. The non-disclosure agreement, rules of behavior, or equivalent documents shall outline the authorized purposes for which the SSA may use NDNH information, the privacy and security safeguards contained in this agreement and security addendum, and the civil and criminal penalties for unauthorized use. SSA may use "wet" and/or electronic signatures to acknowledge non-disclosure agreements, rules of behavior, or equivalent documents.

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

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

6. SSA shall maintain records of authorized personnel with access to NDNH

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

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

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

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

   OCSE has appropriate procedures in place to report security or privacy incidents, or suspected incidents involving the agency input files. Immediately upon discovery, but in no case later than one hour after discovery of the incident, OCSE will report confirmed and suspected incidents to the SSA security contact designated in this security addendum. The requirement for OCSE to report confirmed or suspected incidents to SSA exists in addition to, not in lieu of, requirements to report to US-CERT or other reporting agencies.

   Policy/Requirements Traceability: OMB Circular A130 - Appendix I; OMB M-17-12; NIST SP 800-53 Rev 4, IR-6

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

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

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

9. SSA shall require that personnel accessing NDNH information remotely (for example, telecommuting) adhere to all the security and privacy safeguarding requirements provided in this security addendum. SSA and non-SSA furnished equipment shall have appropriate software with the latest updates to protect against

attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Before electronic connection to SSA resources, SSA shall scan the SSA and non-SSA furnished equipment to ensure compliance with SSA standards. All remote connections shall be through Network Access Control and all data in transit between the remote location and SSA shall be encrypted using FIPS 140-2 encryption standards. Personally owned devices shall not be authorized. See numbers 8 and 19 of this section for additional information.

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

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

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

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

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

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

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

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

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

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

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

13. SSA shall maintain a plan of action and milestones (and when applicable, a corrective action plan) for the information system housing NDNH information to document plans to correct weaknesses identified during security control assessments and to reduce or eliminate known vulnerabilities in the system. SSA shall update the plan of action and milestones (and when applicable, the corrective action plan) as necessary based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

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

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

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

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

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

15. SSA shall limit and control logical and physical access to NDNH information to only those personnel authorized for such access based on their official duties, and identified in the records maintained by SSA pursuant to numbers 6 and 27 of this section. SSA shall prevent personnel from browsing by using technical controls or other compensating controls.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    OCSE does not extract information from the agency input files.

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

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

    OCSE utilizes a time-out function for remote access and mobile devices that requires

a user to re-authenticate after no more than 30 minutes of inactivity.

Policy/Requirements Traceability: OMB M-17-12, NIST SP 800-53 Rev 4, AC-11, AC-12, AC-17, SC-10

23. SSA shall erase electronic records after completing authorized use in accordance with the retention and disposition requirements in the agreement.

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

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

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

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

25. SSA shall implement a Network Access Control (also known as Network Admission Control (NAC)) solution in conjunction with a Virtual Private Network (VPN) option to enforce security policy compliance on all SSA and non-SSA remote devices that attempt to gain access to, or use, NDNH information. SSA shall use a NAC solution to authenticate, authorize, evaluate, and remediate remote wired and wireless users before they can access the network. The implemented NAC solution shall evaluate whether remote machines are compliant with security policies through host(s) integrity tests against predefined templates, such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the SSA enterprise environment. SSA shall disable functionality that allows automatic code execution. The solution shall enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the SSA network and resources while maintaining an audit record on users' access and presence on the SSA network. See numbers 8 and 19 of this section for additional information.

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

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

26. SSA shall ensure that the organization responsible for the data processing facility storing, transmitting, or processing NDNH information complies with the security requirements established in this security addendum. The "data processing facility" includes the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information, and the information systems of SSA

including, but not limited to, employees and contractors working with the data processing facility, contractor data centers, and any other individual or entity collecting, storing, transmitting, or processing NDNH information.

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

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

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

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

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

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

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

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

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

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

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

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

OCSE uses locks and other protective measures at all physical access points (including designated entry/exit points) to prevent unauthorized access to computer and support areas.

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

IV. CLOUD SOLUTION (OPTIONAL)

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

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

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

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

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

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

V. BREACH REPORTING AND NOTIFICATION RESPONSIBILITY

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

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

VI. SECURITY AUTHORIZATION

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

1. SSA Security Posture

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

The SSA ATO was signed on October 11, 2018. OCSE considers the evidence that the SSA environment is in compliance with the security requirements in this security addendum. The effective period for an ATO is three years, which means OCSE maintains the right to request an updated ATO signature if the signature date on file expires during this agreement.

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

2. SSA Permitted Entity Security Posture

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

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

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

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

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

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

By signing the security addendum, SSA signatories confirm that SSA has reviewed the entities specified in the agreement, reviewed the security controls in place to safeguard information and information systems, and has determined that the risk to federal data is at an acceptable level. The security controls in place at all entities specified in the agreement are commensurate with those of a federal system categorized as "moderate" according to FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2002). *See also* OMB M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, November 4, 2016.

VII.   AUDIT REQUIREMENTS

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

Policy/Requirements Traceability: OMB M-17-05, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements, October 25, 2018*; OMB Circular No. A-130, Appendix I

VIII. PERSONS TO CONTACT

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

        Venkata Kondapolu, Acting Director
        Division of Federal Systems
        Office of Child Support Enforcement
        Administration for Children and Families
        Mary E. Switzer Building
        330 C Street, SW, 5th Floor
        Washington, DC 20201
        Phone: 202-260-4712
        Fax: 202-401-5558
        E-mail: Venkata.kondapolu@acf.hhs.gov

    B.   The Social Security Administration contact is:

        Jennifer Rutz, Director
        Division of Compliance and Oversight
        Office of Information Security
        Office of Systems
        Suite 3383 Perimeter East Building
        6401 Security Boulevard
        Baltimore, MD 21235-6401
        Phone: 410-965-0266
        E-mail: Jennifer.Rutz@ssa.gov

IX. 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 shall be binding or recognized, and hereby commit their respective organizations to the terms of this agreement.

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

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

/s/	
Venkata Kondapolu Acting Director Division of Federal Systems Office of Child Support Enforcement	**Date** 1/9/2020
/s/	
Scott M. Lekan Commissioner Office of Child Support Enforcement	**Date** 1/13/2020

B. Social Security Administration

/s/	
Jennifer Rutz Director Division of Compliance and Assessments Office of Information Security	**Date** 1/14/2020

/s/	
Mary Ann Zimmerman Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	**Date** 1/14/2020

APPENDIX A

Background: Current Agreements Between OCSE 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 Enforcement (OCSE) and the Social Security Administration (SSA). OCSE is required to provide SSA with information from the National Directory of New Hires (NDNH). Information exchanges have been ongoing for a number of years.

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 Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match # 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 Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match # 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 Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match # 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 Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match # 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 Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match # 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 Social Security Administration (SSA) and the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services (SSA Match # 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

OCSE 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 OCSE, 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

Cost Benefit Analysis for
Medicare Part D Matching Operation between
Social Security Administration (SSA) and the Office of Child Support Enforcement
(OCSE) (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 Part D premium. 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 redetermination subsidy application data for beneficiaries who have matching income or resource data from SSA and OCSE.

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

The total FY 2018 personnel and computer costs for this matching operation is **$903,500.**

Key Element 1: Personnel Costs
For Agencies –
- Source Agency (OCSE) – N/A
- Recipient Agency (SSA)

    FO Development

This CBA focuses on the cost-savings gained by eliminating field office (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.

- Justice Agency – (N/A)

For Clients – N/A
For Third Parties – N/A
For the General Public – N/A

Key Element 2: Agencies' Computer Costs
For Agencies -
- Source Agency (OCSE) – N/A
- Recipient Agencies (SSA)

  For FY 2018, the Office of Systems reports a computer cost of **$9,500**.

- Justice Agencies – N/A

Interagency Agreement Cost
For FY 2018, the total cost of the IAA for this matching operation is **$894,000**.

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 2018, the total benefits realized from this matching operation is approximately **$15,909,954.**

Key Element 3: Avoidance of Future Improper Payments
To Agencies –
- Source Agency (OCSE) – 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 (OCSE) – 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 **17.6:1.** Therefore, we recommend the continuation of this matching operation.

Cost Benefit Analysis For The Computer Matching Operation #1306 SSA and OCSE

Number of Initial Application Verifications Avoided[1]	495,884
Number of Redetermination Verifications Avoided	16,843
Total Number of Verifications Avoided	512,727
Salary	$100,467[2]
Overhead	1.81[3]

Cost Summary

Interagency Agreement (Based on FY 2018)	$894,000
Systems Costs (Office of Systems, Budget Staff)	$9,500
Total Costs	**$903,500**

Benefit Details

Cost Avoidance of Verification Development	
Development time per **initial application** verification[21] x overhead: 21[4] minutes per verification x 1.81	38.01
Development time per **redetermination v**erification[30] x overhead: 30[5] minutes per verification x 1.81	54.3
(Development time per **initial application** verification x # of verifications)/60 minutes per hour/2080 hours per year = total work years (38.01 x 495884)/60/2080	151.03
(Development time per **redetermination** verification x # of verifications)/60 minutes per hour/2080 hours per year= total work years (54.3 x 16843)/60/2080	7.33
Development cost for **initial application** verification = salary x WY ($100,467 x 151.03)	$15,173,531
Development cost for **redetermination** verification = salary x WY ($100,467 x 7.33)	$736,423
Total development cost avoidance (WY x salary) (rounded)	**$15,909,954**
Benefit-to-Cost Ratio	**17.6:1**

---

[1] SSA avoids verifications when we confirm alleged income/resources through data exchanges. These are the estimated number of verifications avoided by this computer match for initial applications for subsidy and redeterminations of existing subsidies for the period Oct. 2017-Sep. 2018.
[2] FY 2018 Average FO Cost per Work Year (CPWY) includes 20% Fringe Benefits was provided by the Office of Budget.
[3] The overhead rate of 1.81 for the FOs was furnished by the Office of Budget.
[4] The development time of 21 minutes per initial application verification is the estimated average time based on the time it takes to verify an applicant's alleged income/resources against matched data. Source: OPSOS
[5] The development time of 30 minutes per subsidy redetermination verification is the estimated average time based on the time it takes to verify the applicant's alleged income/resources against matched data. Source: OPSOS

Appendix D
Business Needs Assessment Chart
for the Prescription Drug Matching Agreement between OCSE and SSA

SSA Application	Match Method	Function	Elements Provided by SSA to Conduct Match	Elements Provided by OCSE to Conduct Match	SSA User	Elements SSA will update in the OCSEFITM table of the MDB if there is a match	OCSE Databases	Authority
Medicare Data Base (MDB) Office of Child Support Enforcement Data Exchange Request Queue (OCSEQUE) Table	Batch	To determine eligibility of applicants for Extra Help (low-income subsidy assistance) under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003	Client's Own Social Security 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 Unemployment Insurance File: unemployment insurance record identifier, processed date, SSN, verification request code, name, address, unemployment insurance benefit amount, reporting period, transmitter agency code, transmitter state code, and state or agency name.	SSA claims personnel are responsible for determining eligibility for Extra Help.	Quarterly wage record identifier, name, SSN, processed date, address (es), wage amount, quarterly wage reporting period. Employers name, transmitted agency code employer address (es). Unemployment insurance record identifier, processed date, unemployment insurance benefit amount, and reporting period.	National Directory of New Hires (NDNH) - Quarterly Wage File and Unemployment Information File	42 U.S.C. § 653(j)(4), 42 U.S.C. § 1383(f), and 42 U.S.C. §1395w-114(a)(3)(B)