

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 # 1407**

I. PURPOSE

This computer matching agreement, hereinafter “agreement,” governs a matching program between the Office of Child Support Enforcement (OCSE) and the Social Security Administration (SSA). The agreement covers information exchange operations between OCSE and SSA that will provide SSA with quarterly wage and unemployment insurance 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 of 1974, as amended, 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.

II. RESPONSIBILITIES OF THE PARTIES

A. OCSE Responsibilities

1. On a daily basis, OCSE will compare the SSA finder file against the quarterly wage and unemployment insurance 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.

B. SSA Responsibilities

1. On a daily basis, SSA will submit a finder file containing all Clients' Own Social Security Numbers (COSSN) from the Office of Child Support Enforcement Data Exchange Request Queue (OCSEQUE) table contained within the Medicare Data Base (MDB) to OCSE.
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.

III. LEGAL AUTHORITY

The legal authorities for disclosures under this agreement are the Social Security Act (Act) and the applicable routine uses published in the SSA and OCSE System of Records Notices as required by 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)(B). 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 under section 1396u-5(a) or by the Commissioner of Social Security. 42 U.S.C. §1395w-114(a)(3)(B).

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

IV. JUSTIFICATION FOR THE MATCHING PROGRAM AND ITS ANTICIPATED RESULTS

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

A. The Justification for the Matching Program

The NDNH is the only nationally centralized directory of new hire, quarterly wage, and unemployment insurance information, and, as such, provides an effective, efficient, and comprehensive method of collecting and comparing this information. SSA's use of NDNH information supports program accuracy and 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. 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.

B. Anticipated Results of the Matching Program

The matching program reduces the enrollment burden on Medicare beneficiaries and expedites the enrollment process. Additionally this matching program ensures a correct Extra Help determination while reducing the level of effort SSA field offices expend to manually verify all income and resource allegations on the initial Extra Help application and during subsequent eligibility redeterminations. Field offices perform fewer manual verifications when data exchanges verify alleged income.

From October 2012 to September 2013, SSA reduced its workload by 45,512 manual verifications due to this computer match, resulting in an estimated savings of \$1,305,609. SSA estimates the cost of matching with OCSE in fiscal year 2013 was \$458,878. The benefit-to-cost ratio for this matching operation is 2.85:1.

V. DESCRIPTION OF THE MATCHED RECORDS

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. OCSE and SSA Systems of Records (SOR)

OCSE and SSA published notice of the relevant system of records in the *Federal Register*.

SSA collects and maintains this information in the Medicare Database (MDB) system of records, No. 60-0321, published at 69 FR 77816 (December 28, 2004) and 71 FR 42159-42164 (July 25, 2006). The MDB contains information related to Medicare Part A, Part B, Medicare Advantage Part C, and Medicare Part D.

OCSE will match SSA information in the MDB against the quarterly wage and unemployment insurance information furnished by state and federal agencies maintained in its system of records "OCSE National Directory of New Hires" (NDNH), No. 09-80-0381, established by publication in the *Federal Register* on January 5, 2011 at 76 FR 560. Routine use (#9) of the SOR authorizes disclosure of NDNH information to SSA, 76 FR 560, 562 (January 5, 2011).

B. Data Elements Used in the Matching Program

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 quarterly wage file:

- Quarterly wage record identifier
- For employees:
 - (1) Name (first, middle, last)
 - (2) SSN
 - (3) Verification request code
 - (4) Processed date

- (5) Non-verifiable indicator
- (6) Wage amount
- (7) Reporting period
- For employers of individuals in the quarterly wage file of the NDNH:
 - (1) Name
 - (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 unemployment insurance file:

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

4. Data Elements SSA updates in the OCSEFITM 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) Unemployment insurance benefit amount
 - (3) Reporting period
 - (4) Transmitter State Name

C. Number of Records to be Matched

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, we have 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 1.40 billion new hire, quarterly wage, and unemployment insurance 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 the available data elements from the quarterly wage and unemployment insurance files, if any, pertaining to the individuals whose records are contained in the SSA finder file. 42 U.S.C. §653(j)(4).

D. Period of the Matching Program

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

VI. NOTICE PROCEDURES

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

This requirement is best accomplished by direct notice by a statement pursuant to the Privacy Act. 5 U.S.C. §552a(e)(3). SSA and OCSE provide the following additional notices, respectively, to persons whose records are disclosed from the systems of records involved in the matching program established under this agreement.

A. Notice to the General Public

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

B. Notice to Applicants

SSA will notify individuals at the time of application for 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.

VII. VERIFICATION AND OPPORTUNITY TO CONTEST

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

A. Verification of Information Produced in the Matching Program

SSA verifies the name/SSN combinations in its systems of records. SSA will compare the identity 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 quarterly wage information to confirm the information shown by the comparison results, and the appropriate source agency to confirm the unemployment insurance 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 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 responds to contest 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.

VIII. ACCURACY ASSESSMENTS

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

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 NUMIDENT file, in accordance with section 453(j)(1)(A) and (B) of the Act. 42 U.S.C. §653(j)(a)(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 NUMIDENT.

One hundred percent of the employee name and SSN combinations contained in the new hire and the unemployment insurance files against which finder files are compared have been verified against SSA NUMIDENT. For quarterly wage, only 77 percent of the incoming data has a verified name and SSN combination, since some states and employers do not capture enough name information in their records to complete this process. However, information comparisons may be conducted and reliable results obtained.

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

IX. LIMITATIONS ON ACCESS AND USE

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

The Privacy Act also requires that each matching agreement specify procedures governing the use by a recipient agency or non-federal agency of records provided in a matching program by a source agency, including procedures governing return of 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 limitation on the use of the information contained in the finder files disclosed 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 of OCSE, without the written approval of SSA, except as necessary within OCSE for backup to ongoing operations of the matching program. SSA will not grant such authority unless the disclosure is required by law or is essential to the matching program. The SSA finder files remain the property of SSA and are handled as provided in sections X and XI, 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, Duplication, and Rediscovery 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 or disseminated within or outside SSA without the written permission of OCSE, except as necessary within SSA for backup to 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 X and XI once the matching activity authorized under this agreement is complete.

X. PROCEDURES FOR RETENTION AND TIMELY DESTRUCTION OF RECORDS

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

This section specifies the retention periods for the records contained in the SSA finder file and the NDNH records provided to SSA. After the retention periods, 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 the 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 field office 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 system of records concerning individuals in the matching program, other than SSA records needed for integrity and audit purposes. Both SSA and OCSE will keep an accurate accounting of disclosures from an individual's records as required by subsection (c) of the Privacy Act.

XI. PROCEDURES FOR SECURITY

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

SSA and OCSE will comply with the requirements of the Federal Information Security Management Act (FISMA), 44 U.S.C. §3541 et seq.; related Office of Management and Budget (OMB) circulars and memoranda, such as Circular A-130, Management of Federal Information Resources (Nov. 28, 2000), and Memorandum M-06-16, Protection of Sensitive Agency Information (June 23, 2006); 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 Office of Management and Budget 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 its 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 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"). 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 1-877-697-4889.

B. Breach Notification

SSA follows PII breach notification policies and related procedures as required by OMB M-07-16 (May 22, 2007). Any breach or suspected breach will be reported immediately to US-CERT. SSA must report to US-CERT when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 2) there is a suspected or confirmed breach of PII regardless of the manner in which it may have occurred. If SSA determines that the risk of harm requires notification to affected individuals and/or other remedies, SSA will carry out these remedies without cost to OCSE.

C. 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.

XII. EFFECTIVE DATE, DURATION, MODIFICATION, AND TERMINATION 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). OMB Circular No. A-130, Appendix I, 4 (d) requires agencies to provide a Report of Matching Program, including a copy of the agreement, to the Congressional committees and to Office of Management and Budget.

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); 5 U.S.C. §552a(r); and OMB Circular No. A-130, Appendix I, 4(d).

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 April 1, 2015, the day after the expiration date of the recertification agreement, HHS No. 1203.

Therefore, unless Office of Management and Budget or Congress disapprove the agreement within 40 days of the date of the transmittal letter for the report of the signed matching program, or Office of Management and Budget grants a waiver of 10 days of the 40-day review period, or public comments are received that result in cancellation or deferral of the implementation of the program, this agreement shall be effective no sooner than the later of the following dates:

- April 1, 2015, the day after the expiration date of the recertification agreement, (SSA #1306/HHS #1203);
- 30 days after the date SSA publishes the notice of the matching program in the *Federal Register*; or
- 40 days after the date SSA transmits the report of the matching program to the Committee of Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, and Office of Management and Budget's Office of Information and Regulatory Affairs.

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 Data Integrity Board 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 Data Integrity Board 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 Data Integrity Boards 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 HHS Data Integrity Board and the SSA Data Integrity Board.

D. Termination of the Agreement

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

- SSA does not meet its requirement to reimburse OCSE under section 453(k) of the Act as agreed upon in section XV of this agreement and the fiscal agreements of both SSA and OCSE;
- OCSE has reason to believe that the verification and opportunity to contest requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met pursuant to 5 U.S.C. §552a(q)(1);
- any authorized entity to which NDNH information is redisclosed in accordance with section IX is not complying with any of the terms and provisions in this agreement; or
- the privacy or security of NDNH information is at risk.

Each agency will submit to its Data Integrity Board a copy of any notification of termination.

XIII. PERIODIC REPORTING OF RESULTS OF THE MATCHING PROGRAM

The Office of Management and Budget 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. ACCESS TO RECORDS BY THE COMPTROLLER GENERAL

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

XV. REIMBURSEMENT

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

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.

XVI. DISPUTE RESOLUTION

Disputes related to this agreement over financial or accounting treatment 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://www.fns.treas.gov/tfm/vol1/bull.html>).

XVII. PERSONS TO CONTACT FOR FURTHER INFORMATION

A. SSA Contacts:

Program Policy Issues

Craig Streett, Team Supervisor
Office of Enumeration and Medicare Policy
Office of Income Security Programs
2-R-24 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 965-9793
Fax: (410) 966-5366
Email: Craig.Streett@ssa.gov

Computer Systems Issues

Melanie Burns, Director
ORSIS, DMPT2S
Office of Systems
4817 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 966-0444
Email: Melanie.Burns@ssa.gov

Matching Agreement Issues

Linda Frye, Government Information Specialist
Office of Privacy and Disclosure
Office of the General Counsel
617 Altmeyer Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 966-9555
Fax: (410) 594-0115
Email: Linda.Frye@ssa.gov

Data Exchange Issues

Stephanie Brock, HHS Data Exchange Liaison
Office of Data Exchange and Policy Publications
Office of Retirement and Disability Policy
3655 Annex Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 965-7827
Email: Stephanie.Brock@ssa.gov

Systems Security Issues

Michael G. Johnson, Director
Division of Compliance and Oversight
Office of Information Security
Office of Systems
3105 Annex Building
6401 Security Boulevard
Phone: 410-965-0266
Fax: 410-597-0845
Email: Michael.G.Johnson@ssa.gov

B. OCSE Contacts:

Linda Boyer, Data Access and Security Manager
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
370 L'Enfant Promenade SW, 4th Floor
Washington, DC 20447
Phone: 202-401-5410
Fax: 202-401-5558
Email: Linda.Boyer@acf.hhs.gov

Maureen Henriksen, OCSE Liaison with SSA for Data Exchange
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
3-J-6C Robert M Ball Building
6401 Security Boulevard
Baltimore, MD 21235-6401
Phone: (410) 966-5181
Fax: (410) 966-3147
Email: Maureen.Henriksen@acf.hhs.gov



XVIII. INTEGRATION CLAUSE

This agreement, the Form SSA-429, the OCSE reimbursement agreement, and accompanying appendices prepared and authorized at the start of each fiscal year throughout the life of this agreement constitute the entire agreement of the agencies with respect to its subject matter and supersede all other data exchange agreements between the agencies for the purposes described herein. The agencies 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 Office of Management and Budget directives.


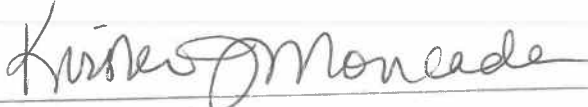
XIX. SIGNATURES

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

OFFICE OF CHILD SUPPORT ENFORCEMENT (OCSE)

	
Vicki Turetsky Commissioner	Date 10/10/14
	
E.J. Holland, Jr. Chairperson HHS Data Integrity Board	Date 12/2/14

SOCIAL SECURITY ADMINISTRATION (SSA)

	
Dawn S. Wiggins Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	Date 10/24/14
	
Kirsten J. Moncada Chair SSA Data Integrity Board	Date 1/16/15

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 # [TBD]

I. PURPOSE AND EFFECT OF THIS SECURITY ADDENDUM

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

By signing this security addendum, OCSE and SSA agree to comply with the provisions of the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), Office of Management and Budget (OMB) directives, and the National Institute of Standards and Technology (NIST) series of Special Publications (SP). 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 (i.e., finder 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, 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, and other machine-readable information, and the information systems of OCSE and SSA and SSA specified entities (i.e., contractors, agents, and other permitted persons) which are hereinafter referred to as “OCSE” and “SSA.”

III. SECURITY AND PRIVACY SAFEGUARDING REQUIREMENTS

This section outlines the safeguarding requirements for receiving NDNH information as well as the safeguards in place at OCSE for protecting the agency finder file. The requirements are drawn from the federal laws and requirements governing the protection of information referenced in Section I of this security addendum as well as the *Office of Child Support Enforcement Division of Federal Systems Security Requirements for Federal Agencies Receiving Federal Parent Locator Service Data*. SSA was provided a copy of the *HHS-OCIO Policy for Information Systems Security and Privacy (IS2P)* and the *Office of Child Support Enforcement Division of Federal Systems Security Requirements for Federal Agencies Receiving Federal Parent Locator Service Data*, on May 19, 2014.

The security requirements to which OCSE and SSA shall ensure compliance and continuously monitor are presented in three categories: administrative, technical, and physical, and three additional sections: Breach Reporting and Notification Responsibility, Security Authorization, and Audit Requirements.

A. ADMINISTRATIVE SECURITY REQUIREMENTS

1. SSA must 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 finder file to authorized personnel who need it to perform their official duties as authorized in this agreement.

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

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

OCSE uses ongoing management oversight and quality assurance capabilities to ensure that only authorized personnel have access to the agency input file.

Policy/Requirements Traceability: Privacy Act 5 U.S.C. § 552a; National Institute of Standards and Technology (NIST) Special Publication (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.

OCSE advises all personnel who will access the agency input file 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: Privacy Act 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 authorized personnel. The training must include information about the responsibility of such personnel for proper use and protection of NDNH information, recognizing and reporting potential indicators of insider threat, and the possible sanctions for misuse. All personnel shall receive security and privacy awareness training prior to accessing NDNH information and at least annually thereafter. Such training shall include instruction covering the other federal laws governing use and misuse of protected information.

OCSE delivers security and privacy awareness training to personnel. The training includes information about the responsibility of such personnel for proper use and protection of other agencies' finder files, recognizing and reporting potential indicators of insider threat, and the possible sanctions for misuse. All personnel receive security and privacy awareness training prior to accessing agency finder files and at least annually thereafter. Such training includes instruction covering the other federal laws governing use and misuse of protected information.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, AT; Federal Information Security Management Act; OMB Circular A-130; OMB M-07-16; NIST SP 800-53 Rev 4, AT-2(2), AT-3

5. SSA personnel with authorized access to the NDNH information shall sign non-disclosure agreements, rules of behavior, or equivalent documents prior to system access annually and if changes occur. The non-disclosure agreement, rules of behavior, or equivalent documents shall outline the authorized purposes for which the NDNH information may be used by SSA 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 file sign non-disclosure agreements and rules of behavior.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, USE; OMB Circular A-130 - Appendix III; OMB M-07-16; NIST SP 800-53 Rev 4, PS-6

6. SSA shall maintain records of authorized personnel with access to the 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 participation in security and privacy awareness training.

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

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

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

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

Policy/Requirements Traceability: *HHS OCIO Policy for IS2PHandbook*, POES

8. 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 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. Prior to electronic connection to SSA resources and at least twice yearly thereafter, SSA shall scan the non-agency furnished equipment to ensure compliance with a set of standards developed by SSA. All connections shall be through a Network Access Control and all data in transit between the remote location and SSA shall be encrypted using Federal Information Processing Standards (FIPS) 140-2 encryption standards. Equipment that may be authorized does not include mobile devices such as PDAs, smartphones, tablets, iPods, MP3 players, or flash drives. See sections II.A.7 and II.B.5 of this security addendum for additional information.

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

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, POES; OMB M-06-16, *Protection of Sensitive Agency Information*; OMB-M-07-16; NIST SP 800-53 Rev 4, AC-17, AC-20

9. SSA shall establish an effective continuous monitoring strategy and implement a continuous monitoring 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 program shall include configuration management, patch management, vulnerability management, the security impact determination of changes to the system and environment, ongoing security control assessments, and reports to SSA officials

as required.

OCSE has established a continuous monitoring 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 file. The program includes configuration management, patch management, vulnerability management, the security impact determination of changes to the system and environment, ongoing security control assessments, and reports to HHS 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*

10. SSA shall have appropriate procedures in place to report security or privacy incidents, or suspected incidents 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 the Federal Parent Locator Service (FPLS) Information Systems Security Officer (ISSO) designated on 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 file. 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 on 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: *HHS OCIO Policy for IS2PHandbook*, IR; OMB Circular A130 – Appendix III; OMB M-07-16; NIST SP 800-53 Rev 4, IR-6

B. TECHNICAL SECURITY REQUIREMENTS

1. SSA shall utilize and maintain technological (logical) access controls that limit access to NDNH information to only those personnel authorized for such access based on their official duties.

OCSE utilizes and maintains technological (logical) access controls that limit access to the agency input file to only those personnel authorized for such access based on their official duties.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook, AC;*
NIST SP 800-53 Rev 4, AC-2

2. SSA shall prevent browsing with technical controls that limit access to NDNH information to assigned cases and areas of responsibility.

OCSE prevents browsing with technical controls that limit access to SSA finder file to authorized personnel.

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

3. SSA shall transmit and store all NDNH information provided pursuant to the agreement in a manner that safeguards the information and prohibits unauthorized access. All electronic SSA transmissions of information to SSA and SSA specified entities (i.e., contractors, agents, and other permitted persons) shall be encrypted utilizing a FIPS 140-2 compliant product.

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

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook, MP,*
OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 4 MP-4, SC-8

4. SSA shall copy and store NDNH information (that must be copied to mobile media) only on federally-owned 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 section II.B.5 of this security addendum for additional information.

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

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook, NCRTP;*
OMB M-07-16; FIPS 140-2, *Security Requirements for Cryptographic Modules*

5. SSA shall prohibit the use of digital media and computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, airports) from transmitting and/or storing NDNH information.

OCSE prohibits the use of digital media and computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, airports) from transmitting and/or storing the agency finder file.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook, POES;*
NIST SP 800-53 Rev 4, AC-19(5), CM-8(3)

6. SSA shall prohibit remote access to NDNH information, except through the use of a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication as required by the OMB M-06-16. SSA shall control remote access through a limited number of managed access control points.

OCSE prohibits remote access to the agency finder file except via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication as required by OMB M-06-16.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, RMT, IA OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 4, AC-17, IA-2(11)(12), SC-8

7. SSA shall maintain a fully automated audit trail system with audit records that capture unsuccessful and successful login and logoff attempts, identification and authentication attempts, date and time of system event, type of system event, user account, system account, and service or process responsible for initiating the system event. The audit trail system shall protect data and the audit tool from unauthorized access, modification and deletion and is regularly reviewed/analyzed for indications of inappropriate or unusual activity.

OCSE maintains a fully automated audit trail system with audit records that capture unsuccessful and successful login and logoff attempts, identification and authentication attempts, date and time of system event, type of system event, user account, system account, service or process responsible for initiating the system event. The audit trail system protects data and the audit tool from unauthorized access, modification and deletion and is regularly reviewed/analyzed for indications of inappropriate or unusual activity.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, AU; NIST SP 800-53 Rev 4, AU-2, AU-3, AU-6(1)(3), AU-8, AU-9(4), AU-11

8. SSA shall log each computer-readable data extract from any databases holding NDNH information and verify each extract has been erased within 90 days after completing required use. If use of the extract is still required to accomplish a purpose authorized pursuant to this agreement and complies with the retention and disposition requirements in the agreement, SSA shall request permission, in writing, to keep the extract for a defined period of time, subject to OCSE written approval.

OCSE does not extract information from the agency input file.

Policy/Requirements Traceability: OMB M-06-16; OMB M-07-16

9. 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 sections II.A.7, II.A.8, and II.B.5 of this security addendum 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: *HHS OCIO Policy for IS2P Handbook*, RMT; OMB M-06-16; OMB M-07-16

10. 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: Privacy Act 5 U.S.C. § 552a

11. 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 devices that attempt to gain access to, or use, NDNH information. SSA shall use a NAC solution to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users before they can access the network. The NAC solution chosen or employed shall be capable of evaluating 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. In addition, functionality that allows automatic execution of code shall be disabled. 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/report on users' access and presence on the SSA network. See sections II.A.7 and II.B.5 of this security addendum for additional information.

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

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, S-RMT.1; NIST SP 800-53 Rev 4, AC-17, AC-20, IA-2(11)(12), IA-3

C. PHYSICAL SECURITY REQUIREMENTS

1. SSA must store all NDNH information provided pursuant to this agreement in an area that is physically safe from access by unauthorized persons at all times.

OCSE stores the agency finder file provided pursuant to this agreement in an area that is physically safe from access by unauthorized persons at all times.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook, PE;*
NIST SP 800-53 Rev 4, PE-2, PE-3

2. 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 sensitive 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 sensitive information. OCSE controls access to facilities and systems wherever sensitive information is 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: *HHS OCIO Policy for IS2P Handbook, PE;*
NIST SP 800-53 Rev 4, AC-2, PE-2

3. SSA shall label printed reports containing NDNH information that 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 never transport NDNH information off SSA 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 finder file information.

Policy/Requirements Traceability: *HHS OCIO Policy for Information Systems Security and Privacy (IS2P) Handbook, MP, MS; NIST SP 800-53 Rev 4, MP-3, MP-4, MP-5, MP-6*

4. SSA shall use locks and other protective measures at all physical access points (including designated entry/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: *HHS OCIO Policy for IS2P Handbook, PE;*
NIST SP 800-53 Rev 4, PE-3

IV. BREACH REPORTING AND NOTIFICATION RESPONSIBILITY

SSA shall have appropriate procedures in place to report security or privacy incidents, or suspected incidents involving NDNH information. Confirmed and suspected incidents in either

electronic or physical form must be reported following SSA procedures immediately upon discovery but in no case later than one hour after discovery. The incident or suspected incident must also be reported to the FPLS Information Systems Security Officer (ISSO) designated on this security addendum. The requirement for SSA to report suspected incidents of NDNH information to OCSE exists in addition to, not in lieu of, any SSA requirements to report to US-CERT or other agency.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2PHandbook*, IR 6; OMB Circular A130 – Appendix III; OMB M-06-19; OMB M-07-16; NIST SP 800-53 Rev 4, IR-6

V. 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.

Prior to receipt of NDNH information, entities shall have implemented the minimum security controls required for a system categorized as “moderate” in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

In addition, if applicable, federal agencies that share NDNH information with specified contractors (i.e., agents, private collection agencies, federal creditor agencies, statistical agencies and other permitted persons) must ensure that the specified contractors meet the same safeguarding requirements. The authorizing official of the agency that re-discloses NDNH information to the permitted entities may grant them the authorization.

The authorization process should be completed according to the NIST SP 800-37 Revision 1, as appropriate.

Federal agencies shall comply with NIST SP 800 37 Revision 1, including 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 SSA specified entities’ (i.e., contractors, agents) 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 SSA specified entities (i.e., contractors, agents) are commensurate with those of a federal system categorized as “moderate” according to FIPS 199 (OMB M-08-21).

VI. AUDIT REQUIREMENTS

The Social Security Act, section 453(m)(2) requires that the Secretary of Health and Human Services establish and implement safeguards with respect to the entities established under section 453 designed to restrict access to confidential information to authorized persons, and restrict use of such information to authorized purposes. 42 U.S.C. § 653(m)(2). The Office of Management

and Budget guidance provides that since information security remains the responsibility of the originating agency, procedures should be agreed to in advance that provide for the monitoring over time of the effectiveness of the security controls of the recipient organization. M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*, December 20, 2000. Also see section 453(l)(2) of the Social Security Act. (42 U.S.C. §653(l)(2)) and 5 U.S.C. §552a(e)(10).

VII. PERSONS TO CONTACT

A. The HHS/ACF/OCSE security contact is:

Linda Boyer, FPLS Information System Security Officer
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
370 L'Enfant Promenade, South West, 4th floor
Washington, DC 20447
Phone: (202) 401-5410
Fax: (202) 401-5558
Email: Linda.Boyer@acf.hhs.gov

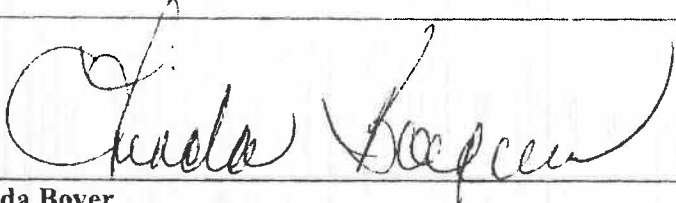
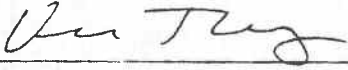
B. The SSA security contact is:

Michael G. Johnson, Director
Division of Compliance and Oversight
Office of Information Security
Office of Systems
3105 Annex Building
6401 Security Boulevard, Baltimore, MD 21235-6401
Phone: 410-965-0266
Fax: 410-966-0527
Email: Michael.G.Johnson@ssa.gov

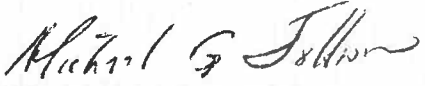
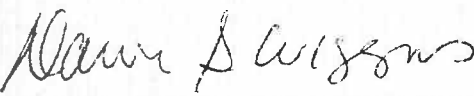
VIII. APPROVALS

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

A. Office of Child Support Enforcement

	
Linda Boyer FPLS Information Systems Security Officer	Date 10-9-14
	
Vicki Turetsky Commissioner	Date 10/10/14

B. Social Security Administration

	
Michael G. Johnson Director Division of Compliance and Oversight Office of Information Security Office of Systems	Date 10-15-14
	
Dawn S. Wiggins Deputy Executive Director Office of Privacy and Disclosure Office of the General Counsel	Date 10-24-14

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 #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 or the District of Columbia, enrolls or seeks enrollment in a prescription drug plan or Medicare Advantage Plan, and who meet 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, the territories, the possessions, and the Commonwealths of Puerto Rico and the Commonwealth of the Northern Mariana Islands.

“Recipient agency” means any agency, or contractor thereof, receiving records contained in a system of records 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 system of records 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

FY13 CBA – Medicare Part D Match 1306 Cost Benefit Analysis for Medicare Part D Matching Program Between SSA and the Office of Child Support Enforcement (OCSE)

The purpose of the matching program is to verify attestations regarding income and resources made by claimants for Medicare Part D prescription drug subsidy assistance under the Medicare Modernization Act of 2003. This CBA report is for the computer matching program between SSA and the OCSE.

The benefit of conducting this matching program is the increased assurance that the agency makes the correct subsidy determination, while reducing the need for field offices to verify all income and resource allegations manually on Medicare Part D subsidy initial applications and redeterminations.

This CBA presents an estimate of the administrative savings due to the cost avoidance. Based on cost avoidance alone, we find this matching program is cost-effective.

The benefit to cost ratio for this matching program is estimated to be 2.85:1. The result supports continuation of this matching program.

Cost Benefit Analysis For The Computer Matching Program (Match #1306) Between SSA And The Office of Child Support Enforcement (OCSE)

Benefits Summary (Verifications Avoided¹)

Number of Initial Application Verifications Avoided	13,733
Number of Redetermination Verifications Avoided	31,779
Total Number of Verifications Avoided	45,512
Total Development Time Avoided (work years)	14.44 WY
Savings per Work Year	\$90,400
Total Benefits	\$1,305,609

Cost Summary

Interagency Agreement (Based on FY 2013)	\$380,178
Systems Costs (Office of Systems, Budget Staff)	\$78,700
Total Costs	\$458,878

Benefit-to-Cost Ratio **2.85 : 1**

Benefit Details

Cost of Verification Development

Development Time per Initial Application Verification² x Overhead³:
21 Minutes per Verification x 1.94 41 minutes/verification

Development Time per Redetermination Verification⁴ x Overhead:
20 Minutes per Verification x 1.94 39 minutes/verification

(Time per Verification x Number of Verifications) ÷ 60 minutes:
(41 minutes x 13,733 verifications) + (39 minutes x 31,779) = 1,802,434/60 30041 work hours

Work Hours ÷ Hours Per Work Year: 29,875 /2080 14.44 WY

Work Years x Salary⁵: 14.36x \$90,400 \$1,305,609

¹ Verifications are avoided when alleged income/resources are confirmed 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 October 2012-September 2013.

² The development time of 21 minutes per initial application is the estimated average time based on the time it takes to verify the applicant's alleged income/resources against matched data. Source: OPSOS

³ The overhead rate of 1.94 for the FOs was furnished by the Office of Budget, DCBFM.

⁴ The development time of 20 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

⁵ FY 2013 Average FO Cost per Work Year (CPWY) includes 20% Fringe Benefits was provided by the Office of Budget.

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

<p>Medicare Data Base (MDB) Office of Child Support Enforcement Data Exchange Request Queue (OCSEQUE) Table</p>	<p>Batch</p>	<p>To determine eligibility of applicants for Extra Help (low-income subsidy assistance) under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003</p>	<p>Client's Own Social Security Number (COSS)(SSN), and Name</p>	<p>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.</p>	<p>SSA claims personnel responsible for determining eligibility for Extra Help.</p>	<p>Quarterly wage record identifier, name, SSN, processed date, address(es), wage amount, quarterly wage reporting period. Employer's name, transmitter agency code, employer address(es). Unemployment insurance record identifier, processed date, unemployment insurance benefit amount, and reporting period.</p>	<p>National Directory of New Hires (NDNH) - Quarterly Wage File and Unemployment Information File</p>	<p>42 U.S.C. §653(j)(4), 42 U.S.C. §1383(f), and 42 U.S.C. §1395w-114(a)(3)(B)</p>
---	--------------	---	--	---	---	---	---	--

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

SSA Application	Method	Function	Elements Provided by SSA to Conduct Match	Elements Provided by OCSE to Conduct Match	SSA User	Elements SSA will update in the OCSEPTIM 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 (OCSEQU) 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, and state or agency name.	SSA claims personnel 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, transmitter 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)