

ATTACHMENT 1

**COMPUTER MATCHING AND PRIVACY
PROTECTION ACT AGREEMENT**

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION
AND
THE HEALTH AND HUMAN SERVICES AGENCY
OF CALIFORNIA

I. Purpose and Legal Authority

A. Purpose

This Computer Matching and Privacy Protection Act (CMPPA) Agreement between the Social Security Administration (SSA) and the California Health and Human Services Agency (State Agency) sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein as "data") made by SSA to the State Agency that administers federally funded benefit programs, including those under various provisions of the Social Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), as well as the state-funded state supplementary payment programs under Title XVI of the Act. The terms and conditions of this Agreement ensure that SSA makes such disclosures of data, and the State Agency uses such disclosed data, in accordance with the requirements of the Privacy Act of 1974, as amended by the CMPPA of 1988, 5 U.S.C. § 552a.

Under section 1137 of the Act, the State Agency is required to use an income and eligibility verification system to administer specified federally funded benefit programs, including the state-funded state supplementary payment programs under Title XVI of the Act. To assist the State Agency in determining entitlement to and eligibility for benefits under those programs, as well as other federally funded benefit programs, SSA discloses certain data about applicants (and in limited circumstances, members of an applicant's household), for state benefits from SSA Privacy Act Systems of Records (SOR) and verifies the Social Security numbers (SSN) of the applicants.

B. Legal Authority

SSA's authority to disclose data and the State Agency's authority to collect, maintain, and use data protected under SSA SORs for specified purposes is:

- Sections 1137, 453, and 1106(b) of the Act (42 U.S.C. §§ 1320b-7, 653, and 1306(b)) (income and eligibility verification data);
- 26 U.S.C. § 6103(l)(7) and (8) (tax return data);
- Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 402(x)(3)(B)(iv)) (prisoner data);

- Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii) (Supplemental Security Income (SSI));
- Section 205(r)(3) of the Act (42 U.S.C. § 405(r)(3)) and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2) (death data);
- Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645) (quarters of coverage data);
- Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA), Pub. L. 111-3 (citizenship data); and
- Routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3) (data necessary to administer other programs compatible with SSA programs).

This Agreement further carries out section 1106(a) of the Act (42 U.S.C. § 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the CMPPA, related Office of Management and Budget (OMB) guidelines, the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3541, et seq.), and related National Institute of Standards and Technology (NIST) guidelines, which provide the requirements that the State Agency must follow with regard to use, treatment, and safeguarding of data.

II. Scope

- A. The State Agency will comply with the terms and conditions of this Agreement and the Privacy Act, as amended by the CMPPA.
- B. The State Agency will execute one or more Information Exchange Agreements (IEA) with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by the State Agency, the data elements that will be disclosed, and the data protection requirements implemented to assist the State Agency in the administration of those programs.
- C. The State Agency will use the SSA data governed by this Agreement to determine entitlement and eligibility of individuals for one or more of the following programs:
 1. Temporary Assistance to Needy Families (TANF) program under Part A of Title IV of the Act;
 2. Medicaid provided under an approved State plan or an approved waiver under Title XIX of the Act;
 3. State Children's Health Insurance Program (CHIP) under Title XXI of the Act, as amended by the Children's Health Insurance Program Reauthorization Act of 2009;

4. Supplemental Nutritional Assistance Program (SNAP) under the Food Stamp Act of 1977 (7 U.S.C. § 2011, et seq.);
5. Women, Infants and Children Program (WIC) under the Child Nutrition Act of 1966 (42 U.S.C. § 1771, et seq.);
6. Medicare Savings Programs (MSP) under 42 U.S.C. § 1396a(10)(E);
7. Unemployment Compensation programs provided under a state law described in section 3304 of the Internal Revenue Code of 1954;
8. Low Income Heating and Energy Assistance (LIHEAP or home energy grants) program under 42 U.S.C. § 8621;
9. State-administered supplementary payments of the type described in section 1616(a) of the Act;
10. Programs under a plan approved under Titles I, X, XIV, or XVI of the Act;
11. Foster Care and Adoption Assistance under Title IV of the Act;
12. Child Support Enforcement programs under section 453 of the Act (42 U.S.C. § 653);
13. Other applicable federally funded programs administered by the State Agency under Titles I, IV, X, XIV, XVI, XVIII, XIX, XX, and XXI of the Act; and
14. Any other federally funded programs administered by the State Agency that are compatible with SSA's programs.

- D. The State Agency will ensure that SSA data disclosed for the specific purpose of administering a particular federally funded benefit program is used only to administer that program.

III. Justification and Expected Results

A. Justification

This Agreement and related data exchanges with the State Agency are necessary for SSA to assist the State Agency in its administration of federally funded benefit programs by providing the data required to accurately determine entitlement and eligibility of individuals for benefits provided under these programs. SSA uses computer technology to transfer the data because it is more economical, efficient, and faster than using manual processes.

B. Expected Results

The State Agency will use the data provided by SSA to improve public service and program efficiency and integrity. The use of SSA data expedites the application process and ensures that benefits are awarded only to applicants that satisfy the State Agency's program criteria. A cost-benefit analysis for the exchange made under this Agreement is not required in accordance with the determination by the SSA Data Integrity Board (DIB) to waive such analysis pursuant to 5 U.S.C. § 552a(u)(4)(B).

IV. Record Description

A. Systems of Records

SSA SORs used for purposes of the subject data exchanges include:

- 60-0058 -- Master Files of SSN Holders and SSN Applications;
- 60-0059 -- Earnings Recording and Self-Employment Income System;
- 60-0090 -- Master Beneficiary Record;
- 60-0103 -- Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB);
- 60-0269 -- Prisoner Update Processing System (PUPS); and
- 60-0321 -- Medicare Part D and Part D Subsidy File.

The State Agency will only use the tax return data contained in **SOR 60-0059** (Earnings Recording and Self-Employment Income System) in accordance with 26 U.S.C. § 6103.

B. Data Elements

Data elements disclosed in computer matching governed by this Agreement are Personally Identifiable Information (PII) from specified SSA SORs, including names, SSNs, addresses, amounts, and other information related to SSA benefits and earnings information. Specific listings of data elements are available at:

<http://www.ssa.gov/dataexchange/>

C. Number of Records Involved

The number of records for each program covered under this Agreement is equal to the number of Title II, Title XVI, or Title XVIII recipients resident in the State as recorded in SSA's Annual Statistical Supplement found on the Internet at:

<http://www.ssa.gov/policy/docs/statcomps/>

This number will fluctuate during the term of this Agreement, corresponding to the number of Title II, Title XVI, and Title XVIII recipients added to, or deleted from, SSA databases.

V. Notice and Opportunity to Contest Procedures

A. Notice to Applicants

The State Agency will notify all individuals who apply for federally funded, state-administered benefits under the Act that any data they provide are subject to verification through computer matching with SSA. The State Agency and SSA

will provide such notice through appropriate language printed on application forms or separate handouts.

B. Notice to Beneficiaries/Recipients/Annuitants

The State Agency will provide notice to beneficiaries, recipients, and annuitants under the programs covered by this Agreement informing them of ongoing computer matching with SSA. SSA will provide such notice through publication in the Federal Register and periodic mailings to all beneficiaries, recipients, and annuitants describing SSA's matching activities.

C. Opportunity to Contest

The State Agency will not terminate, suspend, reduce, deny, or take other adverse action against an applicant for or recipient of federally funded, state-administered benefits based on data disclosed by SSA from its SORs until the individual is notified in writing of the potential adverse action and provided an opportunity to contest the planned action. "Adverse action" means any action that results in a termination, suspension, reduction, or final denial of eligibility, payment, or benefit. Such notices will:

1. Inform the individual of the match findings and the opportunity to contest these findings;
2. Give the individual until the expiration of any time period established for the relevant program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond; and
3. Clearly state that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the SSA data are correct and will effectuate the threatened action or otherwise make the necessary adjustment to the individual's benefit or entitlement.

VI. Records Accuracy Assessment and Verification Procedures

Pursuant to 5 U.S.C. § 552a(p)(1)(A)(ii), SSA's DIB has determined that the State Agency may use SSA's benefit data without independent verification. SSA has independently assessed the accuracy of its benefits data to be more than 99 percent accurate when the benefit record is created.

Prisoner and death data, some of which is not independently verified by SSA, does not have the same degree of accuracy as SSA's benefit data. Therefore, the State

Agency must independently verify these data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

Based on SSA's Office of Quality Performance "FY 2009 Enumeration Quality Review Report #2—The 'Numident' (January 2011)," the SSA Enumeration System database (the Master Files of SSN Holders and SSN Applications System) used for SSN matching is 98 percent accurate for records updated by SSA employees.

Individuals applying for SSNs report their citizenship status at the time they apply for their SSNs. There is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files for a Social Security benefit. The State Agency must independently verify citizenship data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

VII. Disposition and Records Retention of Matched Items

- A. The State Agency will retain all data received from SSA to administer programs governed by this Agreement only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.
- B. The State Agency may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing the State Agency's retention of records.
- C. The State Agency may use any accretions, deletions, or changes to the SSA data governed by this Agreement to update their master files of federally funded, state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing the State Agency's retention of records.
- D. The State Agency may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this Agreement.
- E. SSA will delete electronic data input files received from the State Agency after it processes the applicable match. SSA will retire its data in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

VIII. Security Procedures

The State Agency will comply with the security and safeguarding requirements of the Privacy Act, as amended by the CMPPA, related OMB guidelines, FISMA, related

NIST guidelines, and the current revision of Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, available at <http://www.irs.gov>. In addition, the State Agency will have in place administrative, technical, and physical safeguards for the matched data and results of such matches. Additional administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency, including specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

IX. Records Usage, Duplication, and Rediscovery Restrictions

- A. The State Agency will use and access SSA data and the records created using that data only for the purpose of verifying eligibility for the specific federally funded benefit programs identified in the IEA.
- B. The State Agency will comply with the following limitations on use, duplication, and rediscovery of SSA data:
 1. The State Agency will not use or rediscover the data disclosed by SSA for any purpose other than to determine eligibility for, or the amount of, benefits under the state-administered income/health maintenance programs identified in this Agreement.
 2. The State Agency will not extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs identified in this Agreement. In limited circumstances that are approved by SSA, the State Agency may extract information about an individual other than the applicant/recipient when the applicant/recipient has provided identifying information about the individual and the individual's income or resources affect the applicant's/recipient's eligibility for such program.
 3. The State Agency will not disclose to an applicant/recipient information about another individual (i.e., an applicant's household member) without the written consent from the individual to whom the information pertains.
 4. The State Agency will use the Federal tax information (FTI) disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to section 1137 programs and child support enforcement programs in accordance with 26 U.S.C. § 6103(1)(7) and (8). The State Agency receiving FTI will maintain all FTI from IRS in accordance with 26 U.S.C. § 6103(p)(4) and the IRS Publication 1075. Contractors and agents acting on behalf of the State Agency will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103 and the current revision IRS Publication 1075.

5. The State Agency will use the citizenship status data disclosed by SSA under CHIPRA, Pub. L. 111-3, only for the purpose of determining entitlement to Medicaid and CHIP programs for new applicants.
 6. The State Agency will restrict access to the data disclosed by SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with the purposes identified in this Agreement.
 7. The State Agency will enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties whereby such contractor or agent agrees to abide by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement. The State Agency will provide its contractors and agents with copies of this Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing this Agreement, and thereafter at SSA's request, the State Agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.
 8. The State Agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this Agreement may be subject to civil and criminal sanctions pursuant to applicable Federal statutes.
 9. The State Agency will conduct triennial compliance reviews of its contractor(s) and agent(s) no later than three years after the initial approval of the security certification to SSA. The State Agency will share documentation of its recurring compliance reviews with its contractor(s) and agent(s) with SSA. The State Agency will provide documentation to SSA during its scheduled compliance and certification reviews or upon request.
- C. The State Agency will not duplicate in a separate file or disseminate, without prior written permission from SSA, the data governed by this Agreement for any purpose other than to determine entitlement to, or eligibility for, federally funded benefits. The State Agency proposing the redisclosure must specify in writing to SSA what data are being disclosed, to whom, and the reasons that justify the redisclosure. SSA will not give permission for such redisclosure unless the redisclosure is required by law or essential to the conduct of the matching program and authorized under a routine use. To the extent SSA approves the requested redisclosure, the State Agency will ensure that any entity receiving the redisclosed data will comply with the procedures and limitations on use, duplication, and redisclosure of SSA data, as well as all administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency including specific guidance on safeguarding and reporting

responsibilities for PII, as set forth in this Agreement and the accompanying IEAs.

X. Comptroller General Access

The Comptroller General (the Government Accountability Office) may have access to all records of the State Agency that the Comptroller General deems necessary to monitor and verify compliance with this Agreement in accordance with 5 U.S.C. § 552a(o)(1)(K).

XI. Duration, Modification, and Termination of the Agreement

A. Duration

1. This Agreement is effective from January 1, 2015 (Effective Date) through June 30, 2016 (Expiration Date).
2. In accordance with the CMPPA, SSA will: (a) publish a Computer Matching Notice in the Federal Register at least 30 days prior to the Effective Date; (b) send required notices to the Congressional committees of jurisdiction under 5 U.S.C. § 552a(o)(2)(A)(i) at least 40 days prior to the Effective Date; and (c) send the required report to OMB at least 40 days prior to the Effective Date.
3. Within 3 months prior the Expiration Date, the SSA DIB may, without additional review, renew this Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:
 - the applicable data exchange will continue without any change; and
 - SSA and the State Agency certify to the DIB in writing that the applicable data exchange has been conducted in compliance with this Agreement.
4. If either SSA or the State Agency does not wish to renew this Agreement, it must notify the other party of its intent not to renew at least 3 months prior to the Expiration Date.

B. Modification

Any modification to this Agreement must be in writing, signed by both parties, and approved by the SSA DIB.

C. Termination

The parties may terminate this Agreement at any time upon mutual written consent of both parties. Either party may unilaterally terminate this Agreement upon 90 days advance written notice to the other party; such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow or terminate this Agreement if SSA determines, in its sole discretion, that the State Agency has violated or failed to comply with this Agreement.

XII. Reimbursement

In accordance with section 1106(b) of the Act, the Commissioner of SSA has determined not to charge the State Agency the costs of furnishing the electronic data from the SSA SORs under this Agreement.

XIII. Disclaimer

SSA is not liable for any damages or loss resulting from errors in the data provided to the State Agency under any IEAs governed by this Agreement. Furthermore, SSA is not liable for any damages or loss resulting from the destruction of any materials or data provided by the State Agency.

XIV. Points of Contact

A. SSA Point of Contact

Regional Office

Dolores Dunnachie, Director
San Francisco Regional Office, Center for Programs Support
1221 Nevin Avenue
Richmond CA 94801
Phone: (510) 970-8444 Fax: (510) 970-8101
Dolores.Dunnachie@ssa.gov

B. State Agency Point of Contact

Sonia Herrera
California Health and Human Services Agency
1600 Ninth Street
Sacramento, CA 95814
Phone: (916) 654-3459 Fax: 916-440-5001
Sonia.Herrera@chhs.ca.gov

XV. SSA and Data Integrity Board Approval of Model CMPPA Agreement

The signatories below warrant and represent that they have the competent authority on behalf of SSA to approve the model of this CMPPA Agreement.

SOCIAL SECURITY ADMINISTRATION

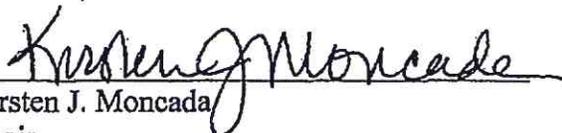


Dawn S. Wiggins
Deputy Executive Director
Office of Privacy and Disclosure
Office of the General Counsel

6-12-14

Date

I certify that the SSA Data Integrity Board approved the model of this CMPPA Agreement.



Kirsten J. Moncada
Chair
SSA Data Integrity Board

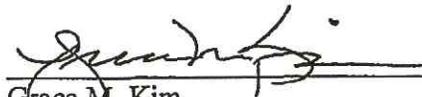
7-2-14

Date

XVI. Authorized Signatures

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

SOCIAL SECURITY ADMINISTRATION

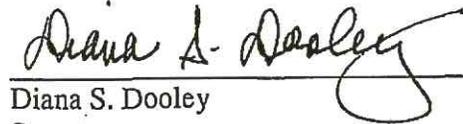


Grace M. Kim
Regional Commissioner
San Francisco

11/6/14

Date

HEALTH AND HUMAN SERVICES AGENCY



Diana S. Dooley
Secretary

October 29, 2014

Date

ATTACHMENT 2

AUTHORIZED DATA EXCHANGE SYSTEM(S)

Attachment 2

Authorized Data Exchange System(s)

BEER (Beneficiary Earnings Exchange Record): Employer data for the last calendar year.

BENDEX (Beneficiary and Earnings Data Exchange): Primary source for Title II eligibility, benefit and demographic data.

LIS (Low-Income Subsidy): Data from the Low-Income Subsidy Application for Medicare Part D beneficiaries -- used for Medicare Savings Programs (MSP).

Medicare 1144 (Outreach): Lists of individuals on SSA roles, who may be eligible for medical assistance for: payment of the cost of Medicare cost-sharing under the Medicaid program pursuant to Sections 1902(a)(10)(E) and 1933 of the Act; transitional assistance under Section 1860D-31(f) of the Act; or premiums and cost-sharing subsidies for low-income individuals under Section 1860D-14 of the Act.

PUPS (Prisoner Update Processing System): Confinement data received from over 2000 state and local institutions (such as jails, prisons, or other penal institutions or correctional facilities) -- PUPS matches the received data with the MBR and SSR benefit data and generates alerts for review/action.

QUARTERS OF COVERAGE (QC): Quarters of Coverage data as assigned and described under Title II of the Act -- The term "quarters of coverage" is also referred to as "credits" or "Social Security credits" in various SSA public information documents, as well as to refer to "qualifying quarters" to determine entitlement to receive Food Stamps.

SDX (SSI State Data Exchange): Primary source of Title XVI eligibility, benefit and demographic data as well as data for Title VIII Special Veterans Benefits (SVB).

SOLQ/SOLQ-I (State On-line Query/State On-line Query-Internet): A real-time online system that provides SSN verification and MBR and SSR benefit data similar to data provided through SVES.

Attachment 2

SVES (State Verification and Exchange System): A batch system that provides SSN verification, MBR benefit information, and SSR information through a uniform data response based on authorized user-initiated queries. The SVES types are divided into five different responses as follows:

- | | |
|----------------------------|---|
| SVES I: | This batch provides strictly SSN verification. |
| SVES I/Citizenship* | This batch provides strictly SSN verification and citizenship data. |
| SVES II: | This batch provides strictly SSN verification and MBR benefit information |
| SVES III: | This batch provides strictly SSN verification and SSR/SVB. |
| SVES IV: | This batch provides SSN verification, MBR benefit information, and SSR/SVB information, which represents all available SVES data. |

** Citizenship status data disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3 is only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants.*



ATTACHMENT 3 OMITTED

SENSITIVE DOCUMENT

ATTACHMENT 4

**ELECTRONIC INFORMATION EXCHANGE SECURITY
REQUIREMENTS AND PROCEDURES**

This document is SENSITIVE and should not be released to the public without prior authorization from DHCS.



**ELECTRONIC INFORMATION EXCHANGE
SECURITY REQUIREMENTS AND PROCEDURES
FOR
STATE AND LOCAL AGENCIES EXCHANGING
ELECTRONIC INFORMATION WITH THE SOCIAL
SECURITY ADMINISTRATION**

SENSITIVE DOCUMENT

**VERSION 6.0.2
April 2014**

Table of Contents

1. **Introduction**
2. **Electronic Information Exchange Definition**
3. **Roles and Responsibilities**
4. **General Systems Security Standards**
5. **Systems Security Requirements**
 - 5.1 **Overview**
 - 5.2 **General System Security Design and Operating Environment**
 - 5.3 **System Access Control**
 - 5.4 **Automated Audit Trail**
 - 5.5 **Personally Identifiable Information**
 - 5.6 **Monitoring and Anomaly Detection**
 - 5.7 **Management Oversight and Quality Assurance**
 - 5.8 **Data and Communications Security**
 - 5.9 **Incident Reporting**
 - 5.10 **Security Awareness and Employee Sanctions**
 - 5.11 **Contractors of Electronic Information Exchange Partners**
6. **General--Security Certification and Compliance Review Programs**
 - 6.1 **The Security Certification Program**
 - 6.2 **Documenting Security Controls in the Security Design Plan**
 - 6.2.1 **When the SDP and Risk Assessment are Required**
 - 6.3 **The Certification Process**
 - 6.4 **The Compliance Review Program and Process**
 - 6.5.1 **FIEP Compliance Review Participation**
 - 6.5.2 **Verification of Audit Samples**
 - 6.6 **Scheduling the Onsite Review**
7. **Additional Definitions**
8. **Regulatory References**
9. **Frequently Asked Questions**
10. **Diagrams**
 - Flow Chart of the OIS Certification Process**
 - Flow Chart of the OIS Compliance Review Process**
 - Compliance Review Decision Matrix**

RECEIVING ELECTRONIC INFORMATION FROM THE SOCIAL SECURITY ADMINISTRATION

1. Introduction ①

The law requires the Social Security Administration (SSA) to maintain oversight and assure the protection of information it provides to its *Electronic Information Exchange Partners* (EIEP). EIEPs are entities that have information exchange agreements with SSA.

The overall aim of this document is twofold. First, to ensure that SSA can properly certify EIEPs as compliant by the SSA security requirements, standards, and procedures expressed in this document before we grant access to SSA information in a production environment. Second, to ensure that EIEPs continue to adequately safeguard electronic information provided to them by SSA.

This document (which SSA considers SENSITIVE¹ and should only be shared with those who need it to ensure SSA-provided information is safeguarded), describes the security requirements, standards, and procedures EIEPs must meet and implement to obtain information from SSA electronically. This document helps EIEPs understand criteria that SSA uses when evaluating and certifying the system design and security features used for electronic access to SSA-provided information.

The addition, elimination, and modification of security control factors determine which level of security and due diligence SSA requires for the EIEP to mitigate risks. The emergence of new threats, attack methods, and the availability of new technology warrants frequent reviews and revisions to our System Security Requirements (SSR). Consequently, EIEPs should expect SSA's System Security Requirements to evolve in concert with the industry.

EIEPs must comply with SSA's most current SSRs to gain access to SSA-provided data. SSA will work with its partners to resolve deficiencies that occur subsequent to, and after, approval for access if updates to our security requirements cause an agency to be noncompliant. EIEPs may proactively ensure their ongoing compliance with the SSRs by periodically requesting the most current SSR package from their SSA contact. Making periodic adjustments is often necessary.

2. Electronic Information Exchange Definition ①

For discussion purposes herein, Electronic Information Exchange (EIE) is any electronic process in which SSA discloses information under its control to any third party for any purpose, without the specific consent of the subject individual or agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the systems of parties to electronic information sharing agreements with SSA. These processes include direct terminal access or DTA to SSA systems, batch processing, and variations thereof (e.g., online query) regardless of the systematic method used to accomplish the activity or to interconnect SSA with the EIEP.

¹ Sensitive data - "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (The Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy but is to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235)."

3. Roles and Responsibilities

The SSA **Office of Information Security (OIS)** has agency-wide responsibility for interpreting, developing, and implementing security policy; providing security and integrity review requirements for all major SSA systems; managing SSA's fraud monitoring and reporting activities; developing and disseminating security training and awareness materials; and providing consultation and support for a variety of agency initiatives. SSA's security reviews ensure that external systems receiving information from SSA are secure and operate in a manner consistent with SSA's Information Technology (IT) security policies and in compliance with the terms of electronic information sharing agreements executed by SSA with outside entities. Within the context of SSA's security policies and the terms of electronic information sharing agreements with SSA's EIEPs, OIS exclusively conducts and brings to closure initial security certifications and periodic security compliance reviews of EIEPs that process, maintain, transmit, or store SSA-provided information in accordance with pertinent Federal requirements which include the following (see also **Regulatory References**):

- a. The **Federal Information Security Management Act (FISMA)** requires the protection of "Federal information in contractor systems, including those systems operated by state and local governments."
- b. The Social Security Administration requires EIEPs to adhere to the policies, standards, procedures, and directives published in this Systems Security Requirements (SSR) document.

Personally Identifiable Information (PII), covered under several Federal laws and statutes, is information about an individual including, but not limited to, personal identifying information including the Social Security Number (SSN).

The data (last 4 digits of the SSN) that SSA provides to its EIEPs for purposes of the Help America Vote Act (HAVA) does not identify a specific individual; therefore, is not "PII" as defined by the Act.

However, SSA is diligent in discharging its responsibility for establishing appropriate administrative, technical, and physical safeguards to ensure the security, confidentiality, and availability of its records and to protect against any anticipated threats or hazards to their security or integrity.

NOTE: Disclosure of Federal Tax Information (FTI) is limited to certain Federal agencies and state programs supported by federal statutes under Sections 1137, 453, and 1106 of the Social Security Act. For information regarding safeguards for protecting FTI, consult IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.

The SSA Regional **Data Exchange Coordinators (DECs)** serve as a bridge between SSA and state EIEPs. In the security arena, DECs assist OIS in coordinating data exchange security review activities with state and local EIEPs; e.g., they provide points of contact with state agencies, assist in setting up security reviews, etc. DECs are also the first points of contact for states if an employee of a state agency or an employee of a state agency's contractor or

agent becomes aware of a suspected or actual loss of SSA-provided Personally Identifiable Information (PII).

4. General Systems Security Standards



EIEPs that request and receive information electronically from SSA must comply with the following general systems security standards concerning access to and control of SSA-provided information.

NOTE: EIEPs may not create separate files or records comprised solely of the information provided by SSA.

- a. EIEPs must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA-provided information neither prevents nor impedes the EIEP's ability to
 - safeguard the information in conformance with SSA requirements,
 - efficiently investigate fraud, data breaches, or security events that involve SSA-provided information, or
 - detect instances of misuse or abuse of SSA-provided information

For example, utilization of cloud computing may have the potential to jeopardize an EIEP's compliance with the terms of their agreement or SSA's associated system security requirements and procedures.

- b. EIEPs must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.
- c. EIEPs must use the software and/or devices provided to the EIEP only in support of the current agreement(s) between the EIEP and SSA.
- d. SSA prohibits modifying any software or devices provided to the EIEPs by SSA.
- e. EIEPs must ensure that SSA-provided information is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in geographic or virtual areas not subject to U.S. law.
- f. EIEPs must restrict access to the information to authorized users who need it to perform their official duties.

NOTE: Contractors and agents (hereafter referred to as contractors) of the EIEP who process, maintain, transmit, or store SSA-provided information are held to the same security requirements as employees of the EIEP. Refer to the section Contractors of Electronic Information Exchange Partners in the Systems Security Requirements for additional information.

- g. EIEPs must store information received from SSA in a manner that, at all times, is physically and electronically secure from access by unauthorized persons.

- h. The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel.
- i. EIEPs must employ both physical and technological safeguards to prevent unauthorized retrieval of SSA-provided information via computer, remote terminal, or other means.
- j. EIEPs must have formal PII incident response procedures. When faced with a security incident caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA-provided information affected by the incident.
- k. EIEPs must have an active and robust employee security awareness program, which is mandatory for all employees who access SSA-provided information.
- l. EIEPs must advise employees with access to SSA-provided information of the confidential nature of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and state laws.
- m. At its discretion, SSA or its designee must have the option to conduct onsite security reviews or make other provisions to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

5. Systems Security Requirements

5.1 Overview

SSA must certify that the EIEP has implemented controls that meet the requirements and work as intended, before we will authorize initiating transactions to and from SSA through batch data exchange processes or online processes such as State Online Query (SOLQ) or Internet SOLQ (SOLQ-I).

The Technical Systems Security Requirements (TSSRs) address management, operational, and technical aspects of security safeguards to ensure only the authorized disclosure and use of SSA-provided information by SSA's EIEPs.

SSA recommends that the EIEP develop and publish a comprehensive Systems Security Policy document that specifically addresses:

- the classification of information processed and stored within the network,
- administrative controls to protect the information stored and processed within the network,
- access to the various systems and subsystems within the network,
- Security Awareness Training,
- Employee Sanctions Policy,

- Incident Response Policy, and
- the disposal of protected information and sensitive documents derived from the system or subsystems on the network.

SSA's systems security requirements represent the current state-of-the-practice security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations, statutes, standards, and guidelines. Additionally, SSA's systems security requirements also include organizationally defined interpretations, policies, and procedures mandated by the authority of the Commissioner of Social Security in areas when or where other cited authorities may be silent or non-specific.

5.2 General System Security Design and Operating Environment

EIEPs must provide descriptions and explanations of their overall system design, configuration, security features, and operational environment and include explanations of how they conform to SSA's requirements. Explanations must include the following:

- Descriptions of the operating environment(s) in which the EIEP will utilize, maintain, and transmit SSA-provided information
- Descriptions of the business process(es) in which the EIEP will use SSA-provided information
- Descriptions of the physical safeguards employed to ensure that unauthorized personnel cannot access SSA-provided information and details of how the EIEP keeps audit information pertaining to the use and access to SSA-provided information and associated applications readily available
- Descriptions of electronic safeguards, methods, and procedures for protecting the EIEP's network infrastructure and for protecting SSA-provided information while in transit, in use within a process or application, and at rest (stored or not in use)
- Descriptions of how the EIEP prevents unauthorized retrieval of SSA-provided information by computer, remote terminal, or other means, including descriptions of security software other than access control software (e.g., security patch and anti-malware software installation and maintenance, etc.)
- Descriptions of how the configurations of devices (e.g., servers, workstations, and portable devices) involving SSA-provided information comply with recognized industry standards and SSA's system security requirements
- Description of how the EIEP implements adequate security controls (e.g., passwords enforcing sufficient construction strength to defeat or minimize risk-based identified vulnerabilities)

5.3 System Access Control

EIEPs must utilize and maintain technological (logical) access controls that limit access to SSA-provided information and associated transactions and functions to only those users, processes acting on behalf of authorized users, or devices (including other information systems) authorized for such access based on their official duties or purpose(s). EIEPs must employ a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or a security software design which is equivalent to such products. The access control software must utilize personal identification numbers (PIN) and passwords or Biometric identifiers in combination with the user's system identification code (userID). The access control software must employ and enforce (1) PIN/password, and/or (2) PIN/biometric identifier, and/or (3) SmartCard/biometric identifier, etc., for authenticating users).

Depending on the computing platform (e.g., client/server (PC), mainframe) and the access software implementation, the terms "PIN" and "user system identification code (userID)" may be, for practical purposes, synonymous. For example, the PIN/password combination may be required for access to an individual's PC after which, the userID/password combination may be required for access to a mainframe application. A biometric identifier may supplant one element in the pair of those combinations. **SSA strongly recommends Two-Factor Authentication.**

The EIEP's implementation of the control software must comply with recognized industry standards. Password policies should enforce sufficient construction strength (length and complexity) to defeat or minimize risk-based identified vulnerabilities and ensure limitations for password repetition. Technical controls should enforce periodic password changes based on a risk-based standard (e.g., maximum password age of 90 days, minimum password age of 3 – 7 days) and enforce automatic disabling of user accounts that have been inactive for a specified period of time (e.g., 90 days).

The EIEP's password policies must also require more stringent password construction (e.g., passwords greater than eight characters in length requiring upper and lower case letters, numbers, and special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

EIEPs must have management control and oversight of the function of authorizing individual user access to SSA-provided information and to oversee the process of issuing and managing access control PINs, passwords, biometric identifiers, etc. for access to the EIEP's system.

The EIEP's systems access rules must cover least privilege and individual accountability. The EIEP's rules should include procedures for access to sensitive information and transactions and functions related to it. Procedures should include control of transactions by permissions module, the assignment and limitation of system privileges, disabling accounts of separated employees (e.g., within 24 hours), individual accountability, work at home, dial-up access, and connecting to the Internet.

5.4 Automated Audit Trail

SSA requires EIEPs to implement and maintain a fully automated audit trail system (ATS). The system must be capable of creating, storing, protecting, and efficiently retrieving and collecting records identifying the individual user who initiates a request for information from SSA or accesses SSA-provided information. At a minimum, individual audit trail records must contain the data needed (including date and time stamps) to associate each query transaction or access to SSA-provided information with its initiator, their action, if any, and the relevant business purpose/process (e.g., SSN verification for Medicaid). Each entry in the audit file must be stored as a separate record, not overlaid by subsequent records. The Audit Trail System must create transaction files to capture all input from interactive internet applications which access or query SSA-provided information.

If a State Transmission Component (STC) handles and audits the EIEP's transactions with SSA, the EIEP is responsible for ensuring that the STC's audit capabilities meet SSA's requirements for an automated audit trail system. The EIEP must also establish a process to obtain specific audit information from the STC regarding the EIEP's SSA transactions.

Access to the audit file must be restricted to authorized users with a "need to know." Audit file data must be unalterable (read-only) and maintained for a minimum of three (preferably seven) years. Information in the audit file must be retrievable by an automated method. EIEPs must have the capability to make audit file information available to SSA upon request. EIEPs must back-up audit trail records on a regular basis to ensure their availability. EIEPs must apply the same level of protection to backup audit files that apply to the original files.

If the EIEP retains SSA-provided information in a database (e.g., Access database, SharePoint, etc.), or if certain data elements within the EIEP's system indicate to users that SSA verified the information, the EIEP's system must also capture an audit trail record of users who viewed SSA-provided information stored within the EIEP's system. The retrieval requirements for SSA-provided information at rest and the retrieval requirements for regular transactions are identical.

5.5 Personally Identifiable Information (PII)

PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. An item such as date and place of birth, mother's maiden name, or father's surname is PII, regardless of whether combined with other data.

SSA defines a **PII loss** as a circumstance when SSA has reason to believe that information on hard copy or in electronic format, which contains PII provided by SSA, left the EIEP's custody or the EIEP disclosed it to an unauthorized individual or entity. PII loss is a reportable incident (refer to **Incident Reporting**).

If a PII loss involving SSA-provided information occurs or is suspected, the EIEP must be able to quantify the extent of the loss and compile a complete list of the individuals potentially affected by the incident (refer to ***Incident Reporting***).

5.6 Monitoring and Anomaly Detection

SSA recommends that EIEPs use an Intrusion Protection System (IPS) or an Intrusion Detection System (IDS). The EIEP must establish and/or maintain continuous monitoring of its network infrastructure and assets to ensure the following:

- The EIEP's security controls continue to be effective over time
- Only authorized individuals, devices, and processes have access to SSA-provided information
- The EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions (i.e., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) as soon as they occur
- The necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes
- Upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk
- In the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions
- The trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are readily discernible

The EIEP's system must include the capability to prevent employees from unauthorized browsing of SSA records. SSA strongly recommends the use of a transaction-driven **permission module design**, whereby employees are unable to initiate transactions not associated with the normal business process. If the EIEP uses such a design, they then need anomaly detection to detect and monitor employee's unauthorized attempts to gain access to SSA-provided information and attempts to obtain information from SSA for clients not in the EIEP's client system. The EIEP should employ measures to ensure the permission module's integrity. Users should not be able to create a bogus case and subsequently delete it in such a way that it goes undetected.

If the EIEP's design does not **currently** use a permission module **and** is not transaction-driven, until at least one of these security features exists, the EIEP must develop and implement **compensating security controls** to deter employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of transactions or queries requested or initiated by individuals and include systematic or manual procedures for verifying that requests and queries of SSA-provided information comply with valid official business purposes. The system must also produce reports that allow management and/or supervisors to monitor user activity, such as the following:

- **User ID Exception Reports:**

This type of report captures information about users who enter incorrect user IDs when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password.

- **Inquiry Match Exception Reports:**

This type of report captures information about users who may be initiating transactions for SSNs that have no client case association within the EIEP's system **(the EIEP's management should review 100 percent of these cases)**.

- **System Error Exception Reports:**

This type of report captures information about users who may not understand or may be violating proper procedures for access to SSA-provided information.

- **Inquiry Activity Statistical Reports:**

This type of report captures information about transaction usage patterns among authorized users and is a tool which enables the EIEP's management to monitor typical usage patterns in contrast to extraordinary usage patterns.

The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

5.7 Management Oversight and Quality Assurance

The EIEP must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA-provided information. They must ensure ongoing compliance with the terms of the EIEP's electronic information sharing agreement with SSA and the SSRs established for access to SSA-provided information. The entity responsible for management oversight must consist of one or more of the EIEP's management officials whose job functions include responsibility to ensure that the EIEP only grants access to the appropriate employees and position types which require SSA-provided information to do their jobs.

The EIEP must ensure that employees granted access to SSA-provided information receive adequate training on the sensitivity of the information, associated safeguards, operating procedures, and the penalties for misuse.

SSA recommends that EIEPs establish the following job functions and require that employees tasked with these job functions do not also share the same job functions as personnel who request or use information from SSA.

- Perform periodic self-reviews to monitor the EIEP's ongoing usage of SSA-provided information.
- Perform random sampling of work activity that involves SSA-provided information to determine if the access and usage comply with SSA's requirements.