INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE NORTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES (STATE AGENCY)

A. PURPOSE: The purpose of this Information Exchange Agreement ("IEA") is to establish terms, conditions, and safeguards under which SSA will disclose to the State Agency certain information, records, or data (herein "data") to assist the State Agency in administering certain federally funded state-administered benefit programs (including state-funded state supplementary payment programs under Title XVI of the Social Security Act) identified in this IEA. By entering into this IEA, the State Agency agrees to comply with:

- the terms and conditions set forth in the Computer Matching and Privacy Protection Act Agreement ("CMPPA Agreement") attached as **Attachment 1**, governing the State Agency's use of the data disclosed from SSA's Privacy Act System of Records; and
- all other terms and conditions set forth in this IEA.

B. PROGRAMS AND DATA EXCHANGE SYSTEMS: (1) The State Agency will use the data received or accessed from SSA under this IEA for the purpose of administering the federally funded, state-administered programs identified in **Table 1** below. In **Table 1**, the State Agency has identified: (a) each federally funded, state-administered program that it administers; and (b) each SSA data exchange system to which the State Agency needs access in order to administer the identified program. The list of SSA's data exchange systems is attached as **Attachment 2**:

TABLE 1

FEDERALLY FUNDED BENEFIT PROGRAMS	
Program	**SSA Data Exchange System(s)**
☒ Medicaid	SDX/BENDEX/SVES IV/EVS/QUARTERS OF COVERAGE/PRISONER QUERY/SOLQ/
☒ Temporary Assistance to Needy Families (TANF) *INCLUDES CHILD CARE SUBSIDY SERVICES	SDX/BENDEX/SVES IV/EVS/QUARTERS OF COVERAGE/PRISONER QUERY/SOLQ
☒ Supplemental Nutrition Assistance Program (SNAP- formally Food Stamps)	SDX/BENDEX/SVES IV/EVS/QUARTERS OF COVERAGE/PRISONER QUERY/SOLQ
☐ Unemployment Compensation (Federal)	
☐ Unemployment Compensation (State)	
☒ State Child Support Agency	SDX/BENDEX
☒ Low-Income Home Energy Assistance Program (LI-HEAP) *INCLUDES EMERGENCY ASSISTANCE, ENERGY ASSISTANCE, CIP	SDX/BENDEX/SVES /EVS/QUARTERS OF COVERAGE

☐ Workers Compensation	
☒ Vocational Rehabilitation Services	SDX/BENDEX/SVES IV/EVS
☐ Foster Care (IV-E)	
☒ State Health Insurance Program (S-CHIP)	SDX/BENDEX/SVESIV/QUARTERS OF COVERAGE/SVES 1 with citizenship/SOLQ
☒ Women, Infants and Children (W.I.C.)	SVES 1
☒ Medicare Savings Programs (MSP)	LIS
☒ Medicare 1144 (Outreach)	MEDOUT 1&2
☒ *Other Federally Funded, State-Administered Programs (List Below)*	
Program	SSA Data Exchange System(s)
CERTAIN DISABLED FOR PRIVATE LIVING ARRANGEMENTS	SDX/BENDEX/SVES /EVS/QUARTERS OF COVERAGE/SOLQ
IN-HOME PAYMENTS FOR MEDICAL ASSISTANCE FOR AGED, DISABLED AND BLIND	SDX/BENDEX/SVES /EVS/QUARTERS OF COVERAGE/SOLQ
M-QB-Q QUALIFIED MEDICARE BENEFICIARIES;MEDICAID PROGRAM PAYS MEDICARE PREMIUMS	SDX/BENDEX/SVES /EVS/QUARTERS OF COVERAGE/SOLQ
BENEFIT DIVISION	SDX/BENDEX/SVES /EVS/QUARTERS OF COVERAGE/SOLQ
STATE PSYCHIATRIC HOSPITALS, DEVELOPMENTAL CENTERS, ALCOHOL AND DRUG ABUSE TREATMENT CENTERS, NEURO-MEDICAL TREATMENTS CENTERS AND SPECIAL SCHOOLS PROGRAM	SDX/BENDEX/SVESIV/EVS
COMMUNITY SERVICES AND SUPPORT PROGRAM TITLE 20, TITLE 19	SDX/BENDEX/SVESIV/EVS
EARLY INTERVENTION PROGRAM	SVES III
INDEPENDENT LIVING SERVICES	SDX/BENDEX/SVES IV/EVS
Division of Aging and Adult Services (DAAS) program	SVES I

(2) The State Agency will use each identified data exchange system ***only*** for the purpose of administering the specific program for which access to the data exchange system is provided. SSA data exchange systems are protected by the Privacy Act and federal law prohibits the use of SSA's data for any purpose other than the purpose of administering the specific program for which such data is disclosed. In particular, the State Agency will use: (a) the **tax return data** 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)(8); and (b) the **citizenship status data** disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3, only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants. The State Agency also acknowledges that SSA's citizenship data may be less than 50 percent current. Applicants for SSNs report their citizenship data 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 a claim for benefits.

C. **PROGRAM QUESTIONNAIRE:** Prior to signing this IEA, the State Agency will complete and submit to SSA a program questionnaire for each of the federally funded, state-administered programs checked in **Table 1** above. SSA will not disclose any data under this IEA until it has received and approved the completed program questionnaire for each of the programs identified in **Table 1** above.

D. **TRANSFER OF DATA:** SSA will transmit the data to the State Agency under this IEA using the data transmission method identified in **Table 2** below:

TABLE 2

TRANSFER OF DATA
☐ Data will be transmitted directly between SSA and the State Agency.
☒Data will be transmitted directly between SSA and NORTH CAROLINA INFORMATION TECHNOLOGY SERVICES (State Transmission/Transfer Component ("STC")) by CYBERFUSION, a secure mechanism approved by SSA. The STC will serve as the conduit between SSA and the State Agency pursuant to the State STC Agreement.
☐ Data will be transmitted directly between SSA and the Interstate Connection Network ("ICON"). ICON is a wide area telecommunications network connecting state agencies that administer the state unemployment insurance laws. When receiving data through ICON, the State Agency will comply with the "Systems Security Requirements for SSA Web Access to SSA Information Through the ICON," attached as **Attachment 3**.

E. **SECURITY PROCEDURES:** The State Agency will comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), and related National Institute of Standards and Technology

guidelines. In addition, the State Agency will comply with SSA's "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration," attached as **Attachment 4**. For any tax return data, the State Agency will also comply with the "Tax Information Security Guidelines for Federal, State and Local Agencies," Publication 1075, published by the Secretary of the Treasury and available at the following Internal Revenue Service (IRS) website: http://www.irs.gov/pub/irs-pdf/p1075.pdf. This IRS Publication 1075 is incorporated by reference into this IEA.

F. **CONTRACTOR/AGENT RESPONSIBILITIES:** The State Agency will restrict access to the data obtained from SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this IEA. At SSA's request, the State Agency will obtain from each of its contractors and agents a current list of the employees of its contractors and agents who have access to SSA data disclosed under this IEA. The State Agency will require its contractors, agents, and all employees of such contractors or agents with authorized access to the SSA data disclosed under this IEA, to comply with the terms and conditions set forth in this IEA, and not to duplicate, disseminate, or disclose such data without obtaining SSA's prior written approval. In addition, the State Agency will comply with the limitations on use, duplication, and redisclosure of SSA data set forth in Section IX. of the CMPPA Agreement, especially with respect to its contractors and agents.

G. **SAFEGUARDING AND REPORTING RESPONSIBILITIES FOR PERSONALLY IDENTIFIABLE INFORMATION ("PII"):**

1. The State Agency will ensure that its employees, contractors, and agents:
   a. properly safeguard PII furnished by SSA under this IEA from loss, theft or inadvertent disclosure;
   b. understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee, contractor, or agent is at his or her regular duty station;
   c. ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected;
   d. send emails containing PII only if encrypted or if to and from addresses that are secure; and
   e. limit disclosure of the information and details relating to a PII loss only to those with a need to know.

2. If an employee of the State Agency or an employee of the State Agency's contractor or agent becomes aware of suspected or actual loss of PII, he or she must immediately contact the State Agency official responsible for Systems Security designated below or his or her delegate. That State Agency official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact identified below. If, for any reason, the responsible State Agency official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the responsible State Agency official or delegate must call SSA's Network Customer Service Center ("NCSC") at 410-965-7777 or toll free at 1-888-772-6661 to report the actual or suspected loss. The responsible State Agency official or delegate will use the worksheet, attached as **Attachment 5**, to quickly gather and organize information about the incident.

The responsible State Agency official or delegate must provide to SSA timely updates as any additional information about the loss of PII becomes available.

3. SSA will make the necessary contact within SSA to file a formal report in accordance with SSA procedures. SSA will notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of PII related to a data exchange under this IEA occurs.

4. If the State Agency experiences a loss or breach of data, it will determine whether or not to provide notice to individuals whose data has been lost of breached and bear any costs associated with the notice or any mitigation.

H. POINTS OF CONTACT:

FOR SSA

Atlanta Regional Office:

Kate Ardoin
Data Exchange Coordinator
BITT
1200 8th Ave North
Birmingham, Al 35285
205 801 1832
(F) 205 801 1804
Kate.ardoin@ssa.gov

Systems Issues:

Pamela Riley
Office of Earnings, Enumeration & Administrative Systems
DIVES/Data Exchange Branch
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-7993
Fax: (410) 966-3147
Email: Pamela.Riley@ssa.gov

Data Exchange Issues:

Guy Fortson
Office of Electronic Information Exchange
GD10 East High Rise
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 597-1103
Fax: (410) 597-0841
Email: guy.fortson@ssa.gov

Systems Security Issues:

Michael G. Johnson
Acting Director
Office of Electronic Information Exchange
Office of Strategic Services
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-0266
Fax: (410) 966-0527
Email: Michael.G.Johnson@ssa.gov

FOR STATE AGENCY

Agreement Issues:

Dale Suggs
Networking Security Specialist
NC DHHS Privacy and Security Office
695 Palmer Drive
Raleigh, NC 27605
(919) 855-3059
(919) 733-1524
Dale.Suggs@dhhs.nc.gov

Technical Issues:

Pyreddy Reddy
Chief Information Security Officer
NC DHHS Privacy and Security Office
695 Palmer Drive
Raleigh, NC 27605
(919) 855-3090
(919) 733-1524
Pyreddy.Reddy@dhhs.nc.gov

I. **DURATION:** The effective date of this IEA is January 1, 2010. This IEA will remain in effect for as long as: (1) a CMPPA Agreement governing this IEA is in effect between SSA and the State or the State Agency; and (2) the State Agency submits a certification in accordance with Section J. below at least 30 days before the expiration and renewal of such CMPPA Agreement.

J. **CERTIFICATION AND PROGRAM CHANGES**: At least 30 days before the expiration and renewal of the State CMPPA Agreement governing this IEA, the State Agency will certify in writing to SSA that: (1) it is in compliance with the terms and conditions of this IEA; (2) the data exchange processes under this IEA have been and will be conducted without change; and (3) it will, upon SSA's request, provide audit reports or other documents that demonstrate review and oversight activities. If there are substantive changes in any of the programs or data exchange processes listed in this IEA, the parties will modify the IEA in accordance with Section K. below and the State Agency will submit for SSA's approval new program questionnaires under Section C. above describing such changes prior to using SSA's data to administer such new or changed program.

K. **MODIFICATION**: Modifications to this IEA must be in writing and agreed to by the parties.

L. **TERMINATION**: The parties may terminate this IEA at any time upon mutual written consent. In addition, either party may unilaterally terminate this IEA 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 under this IEA, or terminate this IEA, if SSA, in its sole discretion, determines that the State Agency (including its employees, contractors, and agents) has: (1) made an unauthorized use or disclosure of SSA-supplied data; or (2) violated or failed to follow the terms and conditions of this IEA or the CMPPA Agreement.

M. **INTEGRATION**: This IEA, including all attachments, constitutes the entire agreement of the parties with respect to its subject matter. There have been no representations, warranties, or promises made outside of this IEA. This IEA shall take precedence over any other document that may be in conflict with it.

ATTACHMENTS

1 – CMPPA Agreement
2 – SSA Data Exchange Systems
3 – Systems Security Requirements for SSA Web Access to SSA Information Through ICON
4 – Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration
5 – PII Loss Reporting Worksheet

N. SSA AUTHORIZED SIGNATURE: The signatory below warrants and represents that he or she has the competent authority on behalf of SSA to enter into the obligations set forth in this IEA.

SOCIAL SECURITY ADMINISTRATION

Michael G. Gallagher
Assistant Deputy Commissioner
for Budget, Finance and Management

5/13/09
Date

O. REGIONAL AND STATE AGENCY SIGNATURES:

SOCIAL SECURITY ADMINISTRATION
REGION IV

Paul Barnes
Regional Commissioner

11/16/09
Date

NORTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES

The signatory below warrants and represents that he or she has the competent authority on behalf of the State Agency to enter into the obligations set forth in this IEA.

Lanier M. Cansler
Secretary

10/30/09
Date

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT BETWEEN THE SOCIAL SECURITY ADMINISTRATION AND THE STATE OF NORTH CAROLINA

TABLE OF CONTENTS

I. Purpose and Legal Authority 3
II. Scope 4
III. Justification and Expected Results 5
IV. Record Description 5
V. Notice and Opportunity to Contest Procedures 6
VI. Records Accuracy Assessment and Verification Procedures 7
VII. Disposition and Records Retention of Matched Items 8
VIII. Security Procedures 8
IX. Records Usage, Duplication, and Redisclosure Restrictions 8
X. Comptroller General Access 10
XI. Duration, Modification, and Termination of the Agreement 10
XII. Reimbursement 11
XIII. Disclaimer 11
XIV. Points of Contact 11
XV. SSA Authorized Signature and Data Integrity Board Approval 11
XVI. Regional and State Signatures 12

I. Purpose and Legal Authority

A. Purpose

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

Under Section 1137 of the Act, the State 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 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 of state benefits from SSA Privacy Act Systems of Records ("SORs") and verifies the Social Security numbers ("SSN") of the applicants.

B. Legal Authority

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

1. Sections 1137, 453, and 1106(b) of the Act (42 U.S.C. §§ 1320b-7, 653, and 1306(b)) (income and eligibility verification data);
2. 26 U.S.C. § 6103(l)(7) and (8) (tax return data);
3. Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 401(x)(3)(B)(iv)) (prisoner data);
4. 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);
5. Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645) (quarters of coverage data);
6. Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3 (citizenship data); and
7. 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 CMPPA 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 Computer Matching and Privacy Protection Act of 1988, 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 must follow with regard to use, treatment, and safeguarding of data.

II. Scope

A. The State will ensure that State Agencies using SSA data to administer federally-funded benefit programs will comply with the terms and conditions of this CMPPA Agreement and the Privacy Act, as amended by the Computer Matching and Privacy Protection Act. For the purpose of this CMPPA Agreement, "State Agencies" do not include any tribal entities recognized by the U.S. Bureau of Indian Affairs.

B. Each State Agency that participates in data exchanges with SSA covered by this CMPPA Agreement will execute one or more Information Exchange Agreements ("IEAs") with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by that 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, through its State Agencies, will use the SSA data governed by this CMPPA Agreement to determine entitlement and eligibility of individuals for the following programs:

1. Temporary Assistance to Needy Families ("TANF") program under Part A of Title IV of the Act;
2. Medicaid provided under a State plan approved 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. Food Stamp 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 Program ("MSP") under 42 U.S.C. § 1320b-14;
7. Unemployment Compensation programs provided under 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 State Agencies under Titles I, IV, X, XIV, XVI, XVIII, XIX, XX, and XXI of the Act; and
14. Any other federally-funded programs administered by State Agencies and are compatible with SSA's programs.

D. The State 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 CMPPA Agreement and related data exchanges with State Agencies are necessary for SSA to assist the State 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

State Agencies 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's program criteria. A cost-benefit analysis for the exchange made under this CMPPA 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:

1. 60-0058 – Master Files of SSN Holders and SSN Applications (accessible through EVS, SVES, or Quarters of Coverage Query data systems);
2. 60-0059 – Earnings Recording and Self-Employment Income System (accessible through BENDEX, SVES, or Quarters of Coverage Query data systems);

3. 60-0090 – Master Beneficiary Record (accessible through BENDEX or SVES data systems);
4. 60-0103 – Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB) (accessible through SDX or SVES data systems);
5. 60-0269 – Prisoner Update Processing System (PUPS) (accessible through SVES or Prisoner Query data systems); and
6. 60-0321 – Medicare Database File.

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

B. Data Elements

Data elements disclosed in computer matching governed by this CMPPA 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/gix/

C. Number of Records Involved

The number of records for each program covered under this CMPPA 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 CMPPA Agreement, corresponding to the number of Title II, Title XVI, and Title XVIII recipients added to or deleted from SSA databases during the term of this CMPPA Agreement.

V. Notice and Opportunity to Contest Procedures

A. Notice to Applicants

State Agencies will notify all individuals who apply for federally-funded, state-administered benefits under the Act that any data they provide is subject to verification through computer matching with SSA. State Agencies and SSA will provide such notice through appropriate language printed on application forms or separate handouts.

B. Notice to Beneficiaries/Recipients/Annuitants

State Agencies will provide notice to beneficiaries, recipients, and annuitants under the programs covered by this CMPPA 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

State Agencies 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 will conclude that the SSA data is 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

State Agencies may use SSA's benefit data without independent verification. SSA has independently assessed the accuracy of its benefits data to be more than 99% accurate when they are 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, State Agencies must independently verify this data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this CMPPA Agreement before taking any adverse action against any individual.

SSA's citizenship data may be less than 50 percent current. Applicants 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 a claim for benefits.

VII. Disposition and Records Retention of Matched Items

A. State Agencies receiving data from SSA to administer programs governed by this CMPPA Agreement will retain all such data only for the required processing times for the applicable federally-funded benefit programs and will then destroy all such data.

B. State Agencies may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing State Agencies' retention of records.

C. State Agencies may use any accretions, deletions, or changes to the SSA data governed by this CMPPA Agreement to update their master files of federally-funded, state-administered benefit program applicants and recipients, which will be retained in accordance with applicable state laws governing State Agencies' retention of records.

D. State Agencies may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this CMPPA Agreement.

E. SSA will delete electronic data input files received from State Agencies 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 will ensure that State Agencies using SSA data comply with the security and safeguarding requirements of the Privacy Act, as amended by the Computer Matching and Privacy Protection Act, related OMB guidelines, the Federal Information Security Management Act of 2002, and related NIST guidelines. In addition, State Agencies using SSA data 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 State Agencies, including specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

IX. Records Usage, Duplication, and Redisclosure Restrictions

A. State Agencies 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. State Agencies will comply with the following limitations on use, duplication, and redisclosure of SSA data:

1. State Agencies will not use or redisclose 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 CMPPA Agreement.
2. State Agencies will not use the data disclosed by SSA to extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs identified in this CMPPA Agreement.
3. State Agencies will use the tax return data 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)(8). Contractors and agents acting on behalf of a State or a State Agency will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103.
4. State Agencies will use the citizenship status data disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3, only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants.
5. State Agencies 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 CMPPA Agreement.
6. State Agencies will enter into a written agreement with each of their 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 CMPPA Agreement. State Agencies will provide their contractors and agents with copies of this CMPPA Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing this CMPPA Agreement, and thereafter at SSA's request, each 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.
7. State Agencies' employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this CMPPA Agreement may be subject to civil and criminal sanctions pursuant to applicable federal statutes.

C. State Agencies will not duplicate in a separate file or disseminate, without prior written permission from SSA, the data governed by this CMPPA Agreement for any purpose other than to determine entitlement or eligibility to federally-funded benefits. A State Agency proposing the redisclosure must specify in writing to SSA what data is 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.

X. Comptroller General Access

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

XI. Duration, Modification, and Termination of the Agreement

A. Duration

1. This CMPPA Agreement is effective from January 1, 2010, ("Effective Date") through June 30, 2011 ("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 the OMB at least 40 days prior to the Effective Date.
3. Within three months prior to the Expiration Date, the SSA DIB may, without additional review, renew this CMPPA Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:
   a. the applicable data exchange will continue without any change; and
   b. SSA and the State certify to the DIB, in writing, that the applicable data exchange has been conducted in compliance with this CMPPA Agreement.
4. If either SSA or the State does not wish to renew this CMPPA Agreement, it must notify the other party of its intent not to renew at least three months prior to the Expiration Date.

B. Modification

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

C. Termination

The parties may terminate this CMPPA Agreement at any time upon mutual written consent of both parties. Either party may unilaterally terminate this CMPPA 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 CMPPA Agreement if SSA determines, in its sole discretion, that the State or a State Agency has violated or failed to comply with this CMPPA Agreement.

XII. Reimbursement

In accordance with Section 1106(b) of the Social Security Act, the Commissioner of SSA has determined not to charge the State and State Agencies the costs of furnishing the electronic data from the SSA SORs under this CMPPA Agreement.

XIII. Disclaimer

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

XIV. Points of Contact

A. SSA Point of Contact
Regional Office
Ardoin, Kate,Data Exchange Coordinator
Birmingham Information Technology Team
1200 8th Ave North
Birmingham, Alabama 35285
Phone: 205-801-1832 / Fax 205-801-1804
Kate.ardoin@ssa.gov

B. State Point of Contact
William M Polk, Deputy General Counsel
Office of the Governor
20301 Mail Service Center
Raleigh, NC 27699-0301
Phone: 919-733-0152 / Fax: 919-733-2120
will.polk@nc.gov

XV. SSA Authorized Signature and Data Integrity Board Approval

The signatory below warrant and represent that he or she has the competent authority on behalf of SSA to enter into the obligations set forth in this CMPPA Agreement.

SOCIAL SECURITY ADMINISTRATION

Michael G. Gallagher
Assistant Deputy Commissioner for Budget, Finance and Management

5/4/2009
Date

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

Mary Glenn-Croft
Chairperson
SSA Data Integrity Board

5/13/09

XVI. Regional and State Signatures

SOCIAL SECURITY ADMINISTRATION

Paul Barnes
Regional Commissioner
Atlanta Region

9/4/09
Date

NORTH CAROLINA

The signatory below warrants and represents that she has the competent authority on behalf of the State to enter into the obligations set forth in this CMPPA Agreement. The signatory below further acknowledges and agrees that, by her signature below, she represents State Agencies and is duly authorized to enter into the obligations set forth in this CMPPA Agreement on behalf of those State Agencies.

Beverly Eaves Perdue
Governor

8/28/09
Date

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.

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

Systems Security Requirements for SWA Access to SSA Information Through the ICON System

8/20/09

Systems Security Requirements for SWA Access to SSA Information Through the ICON System

A. General Systems Security Standards

SWA's that request and receive information from SSA through the ICON system must comply with the following general systems security standards concerning access to and control of SSA information. The SWA must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information retrieved from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The SWA must employ both physical and electronic safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised 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 and State laws. SSA may, at its discretion, make on-site inspections or other provisions to ensure that adequate safeguards are being maintained by the SWA.

B. System Security Requirements for SWA's

SWA's that receive SSA information through the ICON system must comply with the following systems security requirements which must be met before DOL will approve a request from an SWA for online access to SSA information through the ICON system. The SWA system security design and procedures must conform to these requirements. They must be documented by the SWA and subsequently certified by either DOL or by an Independent Verification and Validation (IV&V) contractor prior to initiating transactions to and from SSA through the ICON.

No specific format for submitting this documentation to DOL is required. However, regardless of how it is presented, the information should be submitted to DOL in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the SWA. Written documentation should address each of the following security control areas:

1. General System Security Design and Operating Environment

The SWA must provide a written description of its' system configuration and security features. This should include the following:

a. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and

b. A description of how SSA information will be obtained by and presented to SWA users, including sample computer screen presentation formats and an explanation of whether the SWA system will request information from SSA by means of systems generated or user initiated transactions; and

c. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the SWA system and an explanation of their job descriptions.

Meeting this Requirement

SWA's must explain in their documentation the overall design and security features of their system. During onsite certification, the IV&V contractor, or other certifier, will use the SWA's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and for verifying that the SWA systems and procedures conform to SSA requirements.

Following submission to the DOL in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

2. Automated Audit Trail

SWA's receiving SSA information through the ICON system must implement and maintain a fully automated audit trail system capable of data collection, data retrieval and data storage. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator and relevant business purpose (i.e. the SWA client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored

in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before DOL will approve the SWA's request for access to SSA information through the ICON system.

If SSA-supplied information is retained in the SWA system, or if certain data elements within the SWA system will indicate to users that the information has been verified by SSA, the SWA system also must capture an audit trail record of any user who views SSA information stored within the SWA system. The audit trail requirements for these inquiry transactions are the same as those outlined above for SWA transactions requesting information directly from SSA.

Meeting this Requirement

The SWA must include in their documentation a description of their audit trail capability and a discussion of how it conforms to SSA's requirements. During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the system's audit trail and retrieval capability. The SWA must be able to identify employee's who initiate online requests for SSA information (or, for systems generated transaction designs, the SWA case that triggered the transaction), the time and date of the request, and the purpose for which the transaction was originated. The certifier, or IV&V contractor, also will request a demonstration of the system's audit trail capability for tracking the activity of SWA employees that are permitted to view SSA supplied information within the SWA system, if applicable.

During its future compliance reviews (see below), the SSA also will test the SWA audit trail capability by requesting verification of a sample of transactions it has processed from the SWA after implementation of access to SSA information through the ICON system.

3. System Access Control

The SWA must utilize and maintain technological (logical) access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The SWA must use a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. The SWA must have

management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the SWA system.

Meeting this Requirement

The SWA must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the function responsible for PIN/password issuance and maintenance.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions to verify their responsibilities in the SWA's access control process and will observe a demonstration of the procedures for logging onto the SWA system and for accessing SSA information.

4. **Monitoring and Anomaly Detection**

The SWA's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to an SWA client case (e.g. celebrities, SWA employees, relatives, etc.) If the SWA system design is transaction driven (i.e. employees cannot initiate transactions themselves, rather, the SWA system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an SWA employee unless the SWA system contains a record containing the client's Social Security Number), then the SWA needs only minimal additional monitoring and anomaly detection. If such designs are used, the SWA only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the SWA system by employees not authorized to have access to such information.

If the SWA design does not include either of the security control features described above, then the SWA must develop and implement compensating security controls to prevent their 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 queries requested by individual SWA employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The SWA system must produce reports providing SWA management and/or supervisors with the capability to appropriately monitor user activity, such as:

- User ID exception reports

This type of report captures information about users who enter incorrect user ID's 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 Social Security Numbers that have no client case association within the SWA system.

- System error exception reports

This type of report captures information about users who may not understand or be following proper procedures for access to SSA information through the ICON system.

- Inquiry activity statistical reports

This type of report captures information about transaction usage patterns among authorized users, which would provide SWA management a tool for monitoring typical usage patterns compared to extraordinary usage.

The SWA must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors, or to local security officers, to ensure that the reports are used by those whose responsibilities include monitoring the work of the authorized users.

Meeting this Requirement

The SWA must explain in their documentation how their system design will monitor and/or prevent their employees from browsing SSA information. If the design is based on a "permission module" (see above), a similar design, or is transaction driven (i.e. no employee initiated transactions) then the SWA does not need to implement additional systematic and/or managerial oversight procedures to monitor their employees access to SSA information. The SWA only needs to monitor user access control violations. The documentation should clearly explain how the system design will prevent SWA employees from browsing SSA records.

If the SWA system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an SWA client), then the SWA must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA

information. The SWA should include sample report formats demonstrating their capability to produce the types of reports described above, and the SWA should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the SWA's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the SWA will demonstrate how the system triggers requests for information from SSA.

- If the design is based on a permission module, the SWA will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the SWA system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the SWA system.)

- If the design is based on systematic and/or managerial monitoring and oversight, the SWA will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification, the IV&V contractor, or other certifier, also will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

5. **Management Oversight and Quality Assurance**

The SWA must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information through the ICON system, and to ensure there is ongoing compliance with the terms of the SWA's data exchange agreement with SSA. The management oversight function must consist of one or more SWA management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to

determine whether the requests comply with these guidelines. These functions should be performed by SWA employees whose job functions are separate from those who request or use information from SSA.

Meeting this Requirement

The SWA must document that they will establish and/or maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information, and oversight and monitoring of the use of SSA information within the SWA business process. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

6. **Security Awareness and Employee Sanctions**

The SWA must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other Federal and State laws governing use and misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

Meeting this Requirement

The SWA must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The SWA should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The IV&V contractor, or other certifier, also will meet with a sample of SWA employees to assess their level of training and

understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

7. Data and Communications Security

The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

D. Onsite Systems Security Certification Review

The SWA must obtain and participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the ICON system. DOL will require an initial onsite systems security certification review to be performed by either an independent IV&V contractor, or other DOL approved certifier. The onsite certification will address each of the requirements described above and will include, where appropriate, a demonstration of the SWA's implementation of each requirement. The review will include a walkthrough of the SWA's data center to observe and document physical security safeguards, a demonstration of the SWA's implementation of online access to SSA information through the ICON system, and discussions with managers/supervisors. The IV&V contractor, or other certifier, also will visit at least one of the SWA's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.

The IV&V contractor, or other certifier, will separately document and certify SWA compliance with each SSA security requirement. To fully comply with SSA's security requirements and be certified to connect to SSA through the ICON system, the SWA must submit to DOL a complete package of documentation as described above and a complete certification from an independent IV&V contractor, or other DOL approved certifier, that the SWA system design and infrastructure is in agreement with the SWA documentation and consistent with SSA requirements. Any unresolved or unimplemented security control features must be resolved by the SWA before DOL will authorize their connection to SSA through the ICON system.

Following initial certification and authorization from DOL to connect to SSA through the ICON system, SSA is responsible for future systems security compliance reviews. SSA conducts such reviews approximately once every three years, or as needed if there is a significant change in the SWA's computing platform, or if there is a violation of any of SSA's systems security requirements or an unauthorized disclosure of SSA information by the SWA. The format of those reviews generally consists of

reviewing and updating the SWA compliance with the systems security requirements described above.

ATTACHMENT 4

Information System Security Guidelines For Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration

Social Security Administration
Office of Systems Security Operations Management

Version 3 March 2007

I. Purpose

This document provides security guidelines for Federal, State and Local agencies (hereafter referred to as **'outside entity'**) that obtain information electronically from the Social Security Administration (SSA) through information exchange systems. The guidelines are intended to assist SSA's information exchange partners to understand the criteria SSA will use when evaluating and certifying the system design and security features and protocols used for electronic access to SSA information. The guidelines also will be used as the framework for SSA's compliance review program of its information exchange partners.

II. Role of the SSA Office of Systems Security Operations Management

The SSA Office of Systems Security Operations Management (OSSOM) 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 training and awareness materials and providing consultation and support for a variety of agency initiatives. OSSOM reviews assure external systems that receive information from SSA are secure and operate in a manner that is consistent with SSA's IT security policies and are in compliance with the terms of information sharing agreements executed by SSA and the outside entity. Within the context of these guidelines, OSSOM conducts periodic compliance reviews of outside entities that use, maintain, transmit or store SSA data in accordance with pertinent Federal requirements to include the following:

- The Federal Information Security Management Act (FISMA)
- Social Security Administration (SSA) policies, standards, procedures and directives.

Correspondence should be sent to:

Director, Office of Systems Security Operations Management
Social Security Administration
Room G-D-10 East High Rise
6401 Security Blvd.
Baltimore, MD 21235

You can also send an email to OSSOM.admin@ssa.gov.

III. General Systems Security Standards

Outside entities that request and receive information from SSA through online, overnight, or periodic batch transmissions must comply with the following general

systems security standards concerning access to and control of SSA information. The outside entity must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information received from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The outside entity must employ both physical and technological safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised 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 and State laws. SSA, or its designee will, at SSA's discretion, conduct on-site inspections or make other provisions to ensure that adequate safeguards are being maintained by the outside entity

IV. Technical and Procedural System Security Requirements

Outside entities that receive SSA information must comply with the following technical and procedural systems security requirements which must be met before SSA will approve a request for access to SSA information. The outside entity's system security design and procedures must conform to these requirements. They must be documented by the outside entity and certified by SSA prior to initiating transactions to and from SSA through batch data exchange processes or online processes such as State On Line Query (SOLQ) or Internet SOLQ.

No specific format for submitting security compliance documentation to SSA is required. However, regardless of how it is presented, the information should be submitted to SSA in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the outside entity with authority to certify the organization's intent to comply with SSA requirements. Written documentation should address each of the following security control areas:

A. General System Security Design and Operating Environment

The outside entity must provide a written description of it's' system configuration and security features. This should include the following:

1. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and

2. A description of how SSA information will be obtained by and presented to users, including sample computer screen presentation formats and an explanation of whether the system will request information from SSA by means of systems generated or user initiated transactions; and

3. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the outside entity's system and an explanation of their job descriptions.

Meeting this Requirement

Outside entities must explain in their documentation the overall design and security features of their system. During onsite certification and periodic compliance reviews, SSA will use the outside entity's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and compliance reviews and for verifying that the outside entity's systems and procedures conform to SSA requirements.

Following submission to the SSA in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

B. Automated Audit Trail

Outside entities that receive information electronically from SSA are required to maintain an automated audit trail record identifying either the individual user, or the system process, that initiated a request for information from SSA. (Every request for information from SSA should be traceable to the individual or system process that initiated the transaction.) Outside entities that request information from SSA only through batch selection processes from their client data bases need only keep audit trail records identifying the process that generated the transactions forwarded to SSA. However, if such processes are triggered as a result of user requests initiated from the entity's client data base, then the audit trail record must be able to identify the user who initiated the transaction. The audit trail system must be capable of data collection, data retrieval and data storage. At a minimum, individual audit trail records must contain the data needed to associate each query transaction to its initiator and relevant business purpose (i.e. the outside entity's client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before SSA will approve the outside entity's request for access to SSA information.

If SSA-supplied information is retained in the outside entity's system, or if certain data elements within the outside entity's system will indicate to users that the information has been verified by SSA, the outside entity's system also must capture an audit trail record of any user who views SSA information stored within the outside entity's system. The audit trail requirements for these inquiry transactions are the same as those outlined above for the outside entity's transactions requesting information directly from SSA.
Note: Outside entities that receive SSA information through batch processes must maintain an audit trail, but record retrieval may be either manual or automated. For SOLQ/SOLQ-I, the audit trail must be fully automated, including retrieval of individual audit transaction records.

Meeting this Requirement

The outside entity must include in their documentation a description of their audit trail capability and a discussion of how it conforms to SSA's requirements. During onsite certification and compliance reviews, the SSA, or other certifier, will request a demonstration of the system's audit trail and retrieval capability. The outside entity must be able to identify employees who initiate online requests for SSA information (or, for systems generated transaction designs, the client case that triggered the transaction), the time and date of the request, and the purpose for which the transaction was originated. The certifier will request a demonstration of the system's capability for tracking the activity of employees that are permitted to view SSA supplied information within the outside entity system, if applicable.

During periodic compliance reviews (see below), the SSA also will test the outside entity's audit trail capability by requesting verification of a sample of transactions it has received from the outside entity after implementation of access to SSA information

C. System Access Control

The outside entity must utilize and maintain technological (logical) access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The outside entity must use a

recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. The outside entity must have management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the outside entity's system.

Meeting this Requirement

The outside entity must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the administrative function or official responsible for PIN/password issuance and maintenance.

During onsite certification and compliance reviews, the SSA will meet with the individual(s) responsible for these functions to verify their responsibilities in the outside entity's access control process and will observe a demonstration of the procedures for logging onto the outside entity's system and accessing SSA information.

D. Monitoring and Anomaly Detection

The outside entity's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to a legitimate client case (e.g. celebrities, other employees, relatives, etc.) If the outside entity system design is transaction driven (i.e. employees cannot initiate transactions themselves; rather, the system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an employee unless the client system contains a record containing the client's Social Security Number), then the outside entity needs only minimal additional monitoring and anomaly detection. If such designs are used, the outside entity only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the outside entity system by employees not authorized to have access to such information.

If the outside entity design does not include either of the security control features described above, then the outside entity must develop and implement compensating security controls to prevent their 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 queries requested by individual employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The system must produce reports providing management and/or supervisors with the capability to appropriately monitor user activity, such as:

- User ID exception reports

  This type of report captures information about users who enter incorrect user ID's 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 Social Security Numbers that have no client case association within the outside entity system. **(100% of these cases must be reviewed by management.)**

- System error exception reports

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

- Inquiry activity statistical reports

  This type of report captures information about transaction usage patterns among authorized users, which would provide a tool to the outside entity's management for monitoring typical usage patterns compared to extraordinary usage.

The outside entity must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors, or to local security officers, to ensure that the reports are used by those whose responsibilities include monitoring the work of the authorized users.

Meeting this Requirement

The outside entity must explain in their documentation how their system design will monitor and/or prevent their employees from browsing SSA information. If the design is based on a "permission module" (see above), a similar design, or is transaction driven (i.e. no employee initiated

transactions) then the outside entity does not need to implement additional systematic and/or managerial oversight procedures to monitor their employees access to SSA information. The outside entity only needs to monitor user access control violations. The documentation should clearly explain how the system design will prevent outside entity employees from browsing SSA records.

If the outside entity system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an outside entity client), then the outside entity must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA information. The outside entity should include sample report formats demonstrating their capability to produce the types of reports described above. The outside entity should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification and compliance reviews, the SSA will request a demonstration of the outside entity's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the outside entity will demonstrate how the system triggers requests for information from SSA.

- If the design is based on a permission module, the outside entity will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the outside entity system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the outside entity system.)

- If the design is based on systematic and/or managerial monitoring and oversight, the outside entity will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification and periodic compliance reviews, the SSA will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

E. Management Oversight and Quality Assurance

The outside entity must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information and to ensure there is ongoing compliance with the terms of the outside entity's data exchange agreement with SSA. The management oversight function must consist of one or more outside entity management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to determine whether the requests comply with these guidelines. These functions should be performed by outside entity employees whose job functions are separate from those who request or use information from SSA.

Meeting this Requirement

The outside entity must document that they will establish and maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information, and oversight and monitoring of the use of SSA information within the outside entity's business process. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions.

During onsite certification and compliance reviews, the SSA will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

F. Security Awareness and Employee Sanctions

The outside entity must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other Federal and State laws governing use and

misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

Meeting this Requirement

The outside entity must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The outside entity should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification and periodic compliance reviews, the SSA will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The SSA will also meet with a sample of outside entity employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

G. Data and Communications Security

The outside entity will encrypt all SSN and/or SSN-related information when it is transmitted across dedicated communications circuits between its system, or for intrastate communication among it's local office locations. The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

H. SOLQ/SOLQ-I Onsite Systems Security Certification Review

The outside entity must participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the SOLQ/SOLQ-I system. The onsite certification and compliance reviews will address each of the requirements described above and will include, where appropriate, a demonstration of the outside entity's implementation of each requirement. The review will include a walkthrough of the outside entity's data center to observe and document physical security safeguards, a demonstration of the outside entity's implementation of online

ATTACHMENT 5 09/27/06

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information

1. **Information about the individual making the report to the NCSC:**

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
E-mail Address:					
Check one of the following:					
Management Official		Security Officer		Non-Management	

2. **Information about the data that was lost/stolen:**
   Describe what was lost or stolen (e.g., case file, MBR data):

   Which element(s) of PII did the data contain?

Name		Bank Account Info	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Info	
Place of Birth		Mother's Maiden Name	
Address		Other (describe):	

   Estimated volume of records involved:

3. **How was the data physically stored, packaged and/or contained?**
   Paper or Electronic? (circle one):

   If Electronic, what type of device?

Laptop		Tablet		Backup Tape		Blackberry	
Workstation		Server		CD/DVD		Blackberry Phone #	
Hard Drive		Floppy Disk		USB Drive			
Other (describe):							

Additional Questions if Electronic:

	Yes	No	Not Sure
a. Was the device encrypted?			
b. Was the device password protected?			
c. If a laptop or tablet, was a VPN SmartCard lost?			
Cardholder's Name:			
Cardholder's SSA logon PIN:			
Hardware Make/Model:			
Hardware Serial Number:			

Additional Questions if Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted?			
e. Other circumstances:			

4. **If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NCSC (as listed in #1), information about this employee/contractor:**

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
E-mail Address:					

5. **Circumstances of the loss:**
   a. When was it lost/stolen?

   b. Brief description of how the loss/theft occurred:

   c. When was it reported to SSA management official (date and time)?

6. **Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)**

7. Which reports have been filed? (include FPS, local police, and SSA reports)

Report Filed	Yes	No	Report Number
Federal Protective Service			
Local Police			

	Yes	No
SSA-3114 (Incident Alert)		
SSA-342 (Report of Survey)		
Other (describe)		

8. Other pertinent information (include actions under way, as well as any contacts with other agencies, law enforcement or the press):