DATA ELEMENT	POSITION
Food Stamp Interview Date	1004-1009
Food Stamp Application	1010
Food Stamp Recipient Status	1011
Blank	1012
Onset Date of Disability/Blindness	1013-1020
Disability Payment Code	1021
Drug Addiction or Alcohol Identification Code	1022
Rollback Code	1023
Blank	1024
Welfare ID Number	1025-1046
State Code and Conversion	1047-1048
Special Needs Code	1049
Appeals Decision Date	1050-1057
Blank	1058-1062
Direct Deposit Indicator	1063
Blank	1064
Payee Name and Address Number of Lines	1065
Payee Name and Mailing Address	1066-1197
Payee ZIP Code	1198-1202
Payee ZIP Code + 4	1203-1206
State & County Code of Jurisdiction	1207-1211
District Office (DO) Code	1212-1214
Blank	1215
Blank	1216
Earned Income - Wage Amount	1217-1222
Earned Income - Net Self-Employment Estimate	1223-1228
Blind Work Expense (BWE) Exclusion	1229-1234
Earned Income Exclusion (Plan for Self-support)	1235-1240
Blank	1241
Unearned Income - Number of Occurrences	1242
Unearned Income Type Code ***	1243-1539 (Field 1)

DATA ELEMENT	POSITION
Unearned Income Verification Code ***	1243-1539 (Field 2)
Unearned Income Start Date ***	1243-1539 (Field 3)
Unearned Income Stop Date ***	1243-1539 (Field 4)
Unearned Income Amount ***	1243-1539 (Field 5)
Unearned Income Frequency ***	1243-1539 (Field 6)
Claim or Identification Number For Unearned Income ***	1243-1539 (Field 7)
Blank	1540
Representative (Rep) Payee Indicator	1541
Rep Payee Selection Date	1542-1549
Custody Code	1550-1552
Competency Code	1553
Type of Payee Code	1554-1556
Blank	1557
SSN-Multiple SSN Indicator	1558
SSN-List of Multiple SSNs *	1559-1603
Blank	1604
Residence Address-Number of Lines	1605
Residence Address	1606-1715
Residence ZIP Code	1716-1720
Residence ZIP Code + 4	1721-1724
Blank	1725
Last Transaction Type	1726-1727
Last Transaction Date	1728-1735
Blank	1736
Blank	1737
Advance Payment Indicator	1738
Advance Payment Date	1739-1746

DATA ELEMENT	POSITION
Advance Payment Amount	1747-1751
Blank	1752
Interim Assistance Reimbursement Status Code	1753
State and County Code of Reimbursement	1754-1758
Blank	1759
Payment Date	1760-1767
SSI Gross Payable Amount (Current)	1768-1774
State Gross Payable Amount (Current)	1775-1781
Payment History PHIST Number of Occurrences	1782-1783
PHIST Payment Date ****	1784-1975 (Field 1)
SSI Monthly Assistance Amount ****	1784-1975 (Field 2)
State Supplement Amount ****	1784-1975 (Field 3)
PHIST Payment Payflag 1 ****	1784-1975 (Field 4)
PHIST Payment Payflag 2 ****	1784-1975 (Field 5)
Blank	1976
Overpayment/Underpayment Indicator	1977
Month of Change	1978-1983
Budget Month Flag	1984
Payment Status Code (Current)	1985-1987
Federal Living Arrangement Code	1988
Living Arrangement Code - Optional State Supplement	1989
State and County Code of Jurisdiction (Current)	1990-1994
Concurrent State Payment Code	1995
Medicaid Eligibility Code	1996
Head of Household Indicator	1997
Marital Status	1998
Student Indicator	1999
Earned Income - Net Countable Amount	2000-2005

DATA ELEMENT	POSITION
Unearned Income - Net Countable Amount	2006-2011
SSI Gross Payable Amount	2012-2016
State Gross Payable Amount (Current)	2017-2021
Conditional Payment	2022
Medicaid Test Indicator	2023
Federal Eligibility Code	2024
Optional State Eligibility Code	2025
Mandatory Eligibility Code	2026
Deemed Income Amount	2027-2032
Federal Living Arrangement Code - Budget Month	2033
Earned Income - Retrospective Net Countable Amount	2034-2039
Unearned Income Retrospective Net Countable Amount	2040-2045
Deemed Income Amount Retrospective	2046-2051
40 QQ History	2052-2151

* There could be five occurrences of this information.
** There could be eight occurrences of this information
*** There could be nine occurrences of this information.
**** There could be eight occurrences of this information.

40 QUALIFYING QUARTERS RESPONSE (40 QQ RESPONSE) RECORD LAYOUT - ABRIDGED

DATA ELEMENT	POSITION
Verified SSN	1-9
Input SSN	10-18
Last Name	19-31
First Name	32-41
Middle Initial	42
Date of Birth	43-50
State Code	51-53
State Data	54-75
Minimum Number QQs (1937-1950)	76-77
Maximum Number QQs (1937-1950)	78-79
Railroad Service Months (1937-1946)	80-82
Condition Code	83-84
Qualifying Quarters Pattern (Occurs 89 Times)	85-440

PRISONER RESPONSE RECORD
LAYOUT - ABRIDGED

DATA ELEMENT	POSITION
SVES Prisoner SSN	1-9
SVES Prisoner Name	10-39
SVES State Code	40-42
SVES Welfare ID#	43-64
Status Code	65-66
PUPS SSN	67-75
Last Name	76-95
First Name	96-110
Middle Name	111-125
Suffix	126-129
Prisoner ID Number	130-139
Prisoner Date of Birth	140-147
Sex	148
Date of Confinement	149-156
Release Date	157-164
Report Date	165-172
Prisoner Reporter Name	173-232
Prison/Facility Name	233-292
Prison/Facility Address	293-380
Facility City	381-399
Facility State	400-401
Facility ZIP Code	402-410
Facility Contact Name	411-445
Facility Phone	446-455
Facility FAX #	456-465
Facility Type	466-467
Reserved for Future Use	468-494

Source of **SVES Information:**

The State Verification and Exchange System (SVES) and State Online Query (SOLQ) Manual (*Last revised 02/2007)*

ATTACHMENT C ✓

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 access to SSA information, and discussions with managers/supervisors. The SSA, or other certifier, also will visit at least one of the outside entity'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 SSA will separately document and certify the outside entity's compliance with each SSA security requirement. Any unresolved or unimplemented security control features must be resolved by the outside entity before SSA will authorize their connection to SSA through the SOLQ or SOLQ-I system.

Following a successful security certification review, both parties will sign a document indicating the entity's willingness to comply with these guidelines. Thereafter, the outside entity must participate in a follow-up certification review conducted by SSA after live transmission of online information, and in periodic compliance reviews conducted according to the timeframe established by the information sharing agreement with SSA.

I. Periodic Onsite Compliance Reviews

SSA conducts onsite compliance reviews approximately once every three years, or as needed if there is a significant change in the outside entity'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 outside entity. The format of those reviews generally consists of reviewing and updating the outside entity's compliance with the systems security requirements described above.

ATTACHMENT D

Worksheet for Reporting Loss or Potential Loss
of Personally Identifiable Information (PII)

1. Information about the individual making the report:

Name					
Position					
State Agency/Company					
Phone Numbers					
Work		Cell		Home/Other	
Email Address					
Position Type *(select one)*					
□ 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 Information	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Information	
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 and continue below)*:

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 #			

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 (personal information deleted or blacked out)?			
e. Other *(describe)*			

4. Information about the individual in possession of the data at the time of loss (if same individual as in #1, please indicate "Same as in #1":

Name					
Position					
State Agency/Company					
Phone Numbers:					
Work		Cell		Home/Other	
Email Address					

If person who was in possession of the data or assigned to the data is a contractor employee:

Contractor	
State Agency Contract Identification Number *(if known)*	

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 an SSA management official *(date and time)*?

6. **Have any other SSA components/individuals been contacted? If so, who?** *(include Deputy Commissioner-level, Agency-level, Regional/Associate-level component names)*

Name	SSA Component	Phone Number

7. **What reports have been filed?** (include local police, and SSA reports)

Report Filed	Yes	No	Report Number
Local Police			
Other *(describe)*			