

EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D. C. 20210	CLASSIFICATION
	UI
	CORRESPONDENCE SYMBOL
	OWS/DPM
RESCISSIONS	ISSUE DATE
	March 19, 2004
None	EXPIRATION DATE
	March 31, 2005

ADVISORY : UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 19-04

TO : STATE WORKFORCE AGENCIES

**FROM : CHERYL ATKINSON s/s
 Administrator
 Office of Workforce Security**

SUBJECT : Additional Information for State Workforce Agencies to Implement Data Sharing with the Social Security Administration via the Interstate Connection Network

1. **Purpose.** To provide State Workforce Agencies (SWAs) with additional information and documents to complete the project to exchange data with the Social Security Administration (SSA).
2. **Reference.** Unemployment Insurance Program Letter (UIPL) [No. 29-02](#)
3. **Background.** The U.S. Department of Labor (USDOL) and SSA signed a memorandum of understanding on March 5, 2004, that will allow states to have real-time access to social security data to combat unemployment benefit fraud and abuse. The signing of this agreement clears the way for the SSA and SWAs to proceed with implementation of the data exchange.
4. **Action Required.** The following are next steps for SWAs:
 - SWAs should, if they haven't already, complete the programming and testing necessary to imbed in their automated systems the process to request and receive SSA data. Attached is a copy of the latest program logic document that should be used by the states for that purpose (see attachment I). This document was e-mailed to the Interstate Connection Network (ICON) programmers and to the SWA Interstate Program Coordinators on January 15, 2004.
 - SWAs should ensure that their security systems meet SSA's requirements and that they are ready for the required Independent Verification and Validation (IV&V). Attached are two reference documents. The first document, "[Systems Security Requirements for SWA Access to SSA Information Through the ICON System.](#)" provides SWAs with the SSA security requirements against which the IV&V must be conducted (see attachment II). The SWAs should provide the second document, "[SWA Access to SSA Data through the Interstate Connection Network, IV&V Specifications.](#)" to the IV&V contractor as a guide in conducting the IV&V (see attachment III). In order for a state to be allowed access to the SSA data, the SWA system must meet SSA's security requirements.
 - SWAs should begin working with the SSA regional contacts (see attachment IV) to develop and execute a state-specific data sharing agreement or to amend and execute an existing state-specific data sharing agreement.

SWAs should forward a signed copy of their data sharing agreement with SSA and a copy of their IV&V certification to the National Office through the Regional Office (RO). Both are required to initiate the reciprocal data exchange.

- SWAs that did not submit supplemental budget requests for SSA crossmatch and IV&V activities last year may do so this year. SWAs seeking these funds should contact their RO for information and instructions.
- The Information Technology Support Center (ITSC) is prepared to assist SWAs obtain an IV&V (see attachment V). SWAs may use ITSC services via a direct, separately-funded contract or by the established deobligation procedure.

5. **Inquiries.** Inquiries should be directed to your RO.

6. **Attachments**

- I. [Program Logic Document](#)
- II. [Systems Security Requirements for SWA Access to SSA Information Through the ICON System](#)
- III. [SWA Access to SSA Data Through the Interstate Connection Network, IV&V Specifications](#)
- IV. [SSA Regional Contacts](#)
- V. [ITSC IV&V Proposal](#)



SSA/SWA Data Exchange Project

UIQ

Program Logic Document

Revised as of 01/15/04

UIQ Program Logic Document

	Page
1.0 Scope	
1.1 Identification	4
1.2 System Overview..	4
1.3 Background	5
2.0 System Description.....	6
3.0 Security/Controls	7
4.0 Connectivity.....	9
5.0 Initial Claims Integration.	9
6.0 Stand-Alone Transaction	10
7.0 UIQ Requests.....	11
8.0 UIQ Responses....	14
9.0 SWA Claimstaking Diagram	39
10.0 Impact to SWA.....	40
11.0 ICON Network Diagram...	41
12.0 TCP/IP SWAs	42
Appendix A.	43
Appendix B.	50
Appendix C.	53
Glossary	56

1.0 Scope

1.1 Identification

This Program Logic Document (PLD) applies to the online application of social security information via the Interstate Connection Network (ICON) between State Workforce Agencies (SWAs) and the Social Security Administration (SSA). The application is referred to as UIQ, Unemployment Insurance Query.

1.2 System Overview

This document provides an overview of how SWAs will participate with SSA in the UIQ application.

UIQ is designed to provide SWAs with online access to SSA's information so that the SWA will be able to verify SSN and pension information during the initial claimstaking process.

The UIQ request will be initiated via an automated process that is to be embedded in the initial claimstaking software. The UIQ request is transmitted over the ICON network to the ACS ICON Hub - then routed via a dedicated circuit to the SSA Mainframe. The SSA UIQ response is returned to the SWA over the same path.

The SWAs will sign an agreement directly with SSA to participate in UIQ. In signing the agreement, the SWA is granting SSA access to their IBIQ (Interstate Benefits Inquiry) application. SSA will initiate IBIQ requests with those participating SWAs. The ACS ICON Hub will serve as the traffic cop for this data exchange.

1.3 Background

Currently, the SSA and SWAs are sharing data electronically in a batch environment, usually through the SWA's Health and Human Services Department. There is a need for SSN validation and verification of pension to be available, real-time, during the initial claimstaking process. The U.S. Department of Labor (USDOL) and the Social Security Administration have agreed that SWAs and SSA may exchange online data via the ICON Frame Relay Network, which links the 53 SWAs.

The Social Security Administration would like access to the SWA's IBIQ (Interstate Benefits InQuiry) in order to audit individuals who are receiving SSI benefits. In return for online access to IBIQ data, the SSA is offering an application to the SWAs called UIQ (Unemployment Insurance Query). UIQ will allow SWAs to verify SSN and pension information online against the SSA's information.

Each SWA that wants to participate in the data exchange will sign an agreement with the Social Security Administration. The ACS ICON Hub will serve as a traffic cop, directing the queries and responses from the participating SWAs and rejecting the queries if the SWA is not participating.

The online data sharing between SSA and SWAs will both improve administrative efficiencies and assist in the detection and prevention of overpayments in both programs.

Currently two SWAs (Utah and Wisconsin) validate SSN related data with SSA in a similar application known as SOLQ, State On-Line Query.

2.0 System Description

UIQ will be invoked by imbedding code in the SWA's initial claimstaking software. This code will create a UIQ request to the ACS ICON Hub. The hub software will determine if this SWA is participating with SSA. If so, the request will be forwarded to SSA. SSA will send the response back to the hub. ACS will forward the response back to the requesting SWA.

It is up to the SWA to determine what it wants to do with the SSA response. The SWA will write code to interpret the SSA's response and act accordingly (sending error message or updating record as having been verified, etc).

In addition to the initial claimstaking process, the SWA may develop a stand-alone query to be used only with SSNs needing verification for which there is an initial claim on file. This query's use should be audited and severely limited.

3.0 Security/Controls

Each of the States will be required to sign an individual data sharing agreement with the SSA. This agreement requires that the state will implement procedures to address potential browsing or inappropriate use of SSA information by state employees who have access to this data.

Prior to initiation of the data exchange SSA may audit the state's system and/or procedures to ensure appropriate controls are in place to protect SSA data. These audits may also occur at anytime during the life of the data sharing agreement.

States are required to immediately report breaches of access and disclosure requirements applicable to this UIQ operation to the designated SSA systems security authority. The systems security authority will be designated at the time of signing the data sharing agreement.

Documentation on security safeguards and how they will be addressed within the systems design for UIQ will need to be sent to SSA. The State must maintain a fully automated audit trail to be kept for a period of time specified by SSA's security officer and ensure that each "category" of State employee granted access to SSA records via UIQ has access only to information from UIQ needed to perform their job duties. The State must have in place, as required by SSA, the capability to monitor access to sensitive queries (e.g., public officials, celebrities, etc.) and certify, as required by SSA, that each query was done in conjunction with a valid purpose specified in this agreement. The State must notify SSA of any major change in system platform (hardware and/or software) procedure and/or policy affecting transmission and/or distribution of UIQ information so that a re-review of system safeguards can be initiated.

There are two types of queries that are approved.

- **Initial Claims Query:** This query is done at the time of filing an Initial Claim for UI benefits to verify the identity of the individual (SSN, name & birth date) and to provide information on any SSA benefits being received if the state makes deductions for those benefits. An Initial Claims Query process may be established if it is restricted in the following manner.

States will be required to embed the UIQ code in their initial claims application process so that a SSA query cannot be generated without an Initial Claim being officially filed in the State. Access to the SSA data must also be limited to only those individuals who need access based on their job requirements. These steps are essential in order to exchange data with SSA.

- **Stand-Alone Query:** At some point after an Initial Claim is filed a state may need to verify or re-verify information to resolve an issue with a claim such as change in SSI benefits or pension receipt. The stand-alone query is only to be used to support such verification activities.

The stand-alone query application must also be limited to only SSNs that have a current UI benefit year or a benefit year that ended not more than 12 months prior to the query being requested. A stand-alone query must limit access to specifically identified State employees whose job duties require access.

4.0 Connectivity

The exchange of data between SWAs and SSA will traverse the existing ICON Private Frame Relay Network. To complete the connection to the SSA, a dedicated circuit has been installed linking the ACS ICON Hub to the SSA Mainframe in Baltimore.

It is this connectivity that will handle the flow of data between the SWAs and the SSA.

Due to the use of the existing ICON Network, there will be no additional network/router changes required for any SWA.

5.0 Initial Claims Integration

The SWA Initial Claims process must be modified so the state's system automatically generates a request for SSN and related information validation. This automated SSA verification request will be an additional step in the claimstaking process and will occur for every initial claim.

A UIQ transaction should then be initiated in connection with the initial claimstaking process.

The state's benefit system must also be modified to accept the UIQ response sent from SSA and provide alerts to the initial claimstaking process if there is some type of problem or discrepancy.

UIQ is a direct communication between the respective systems based on processing architecture that will enable the systems to interact without intervening services, data storing or scheduling.

Exchange of information is real-time in the sense that responses to queries are immediate.

6.0 Stand-Alone Transaction

A stand-alone query may be developed by the SWA. This stand-alone query will send the UIQ transaction. It should be used only so that a state may verify a claim on file that was unable to be verified or re-verify the information in order to resolve an issue with a claim.

In creating this, SWAs should keep in mind that an initial claim must be on file in order to send the query. It should be limited to SSNs that have a current UI benefit year or a benefit year that ended not more than 12 months prior to the query being requested. Also, access should be limited to those individuals whose job duties require access.

For security purposes, an audit log of activity must be created. This audit log should contain who sent the inquiry, which SSN was inquired upon, and the date and time of the inquiry. The audit log may be reviewed by SSA.

7.0 UIQ Requests

The transaction for sending a UIQ request is **UIQS**. IBM SWAs will do a Start transaction to the LM hub sysid with the data. The length of the UIQ request is 130 bytes. This includes the UIQ header data elements which will be appended on the front of the UIQ request record. Your UIQ request header will be returned to you if a problem is encountered. The ROSTATUS field will tell you the reason. The UIQ request data elements follow:

UIQ Request Header Data Elements

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
1	Requesting State	A/N	1	2	R	State Postal Code of SWA sending request
2	CICS Applid	A/N	3	8	R	SWA's CICS applid name
3	Today's Date	A/N	11	6	R	Today's Date in YYMMDD format
4	Today's Time	A/N	17	6	R	Today's Time in HHMMSS format
5	Status	N	23	1	R	Status of Request: 0 – Request ok (SWA codes this) Hub may return: 1 – SSA not currently available 2 – SWA is not currently participating 8 – Invalid data from SWA
6	Filler	N	24	1	O	Space

UIQ Request Detail Data Elements

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
7	Input PIN	A/N	25	20	R	Personal Identification Number for SWA inquiry audit purposes
8	SSN	N	45	9	R	Social Security Number inquiring upon
9	CAN/BIC	A/N	54	12	R	Spaces
10	Given Name	A/N	66	5	R	Claimant's First name
11	Middle Initial	A/N	71	1	O	Claimant's Middle Initial
12	Surname	A/N	72	7	R	Claimant's Last Name
13	Date of Birth	N	79	8	R	Claimant's Date of Birth. Format is MMDDCCYY.
14	Sex Code	A/N	87	1	O	F =Female, M =Male, U =Unknown
15	State Agency Code	A/N	88	3	R	The 2-position State Code preceded by a 'U'. Format is Unn with nn being the SWA's State Code. See Appendix C for State Codes.
16	Filler	A/N	91	40	R	Spaces

8.0 UIQ Responses

The transaction that will be sent to SWAs for a UIQ response is **UIQR**. The length will depend on which type of response SWAs are to receive. SWAs should program the response record layout according to whether or not they offset social security pensions from the claimants UI benefits. The Record Type (field 18) will indicate the type of response received.

The Verification Code (field 16) will indicate whether or not the SSN is verified. The Verification SSN Data field (field 17) will contain the data of the differences found.

SWAs receiving the responses using offset will want to interrogate the contents of Fields 79-81. The Monthly Benefit Credited Amount (field 80) is the amount of the check paid to the person. The Monthly Benefit Credited Date (field 79) will hold the date of the occurrence. The Monthly Benefit Credited Type (field 81) will indicate if the benefits were paid or not. These 3 fields reflect the last eight changes in payment, with the most recent change in the first occurrence.

If there is an error such as the record not being on file at SSA, SSA will send back an error response. The error response consists of an error code, the associated error number and an error message. The remaining record is spaces.

Appended to the front of the response from SSA will be the Input PIN and SSN from the request. These two fields, totaling 29 bytes, will be at the front of every UIQ response received.

UIQ Response Precursor

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
1	Input PIN from Request	A/N	1	20	R	Personal Identification Number for SWA inquiry audit purposes taken from request
2	SSN from Request	N	21	9	R	Social Security Number that SWA inquired upon

If there is an error such as the record not being on file at SSA, SSA will send back an error response. The UIQ Response Error Record follows:

UIQ Response Error Record

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
1	Response Error Code	A/N	1	1	R	Values are: E =Error, S=System Error
2	Response Error Number	N	2	3	R	Error number corresponding with message – example '505' means 'error record not in file'. Complete list is in Appendix B
3	Response Error Message	A/N	5	80	R	Description of Error message such as 'error record not in file'. Complete list is in Appendix B
4	Filler	A/N	85	72	R	Spaces

The two types of good responses as received from SSA are described on the following pages:

UIQ Response Record for SWAs not using offset

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
1	SSN	N	1	9	R	Social Security Number inquiring upon
2	CAN/BIC	A/N	10	12	O	Spaces
3	Surname	A/N	22	19	R	Claimant's Last name
4	Middle Initial	A/N	41	1	O	Claimant's Middle Initial
5	Given Name	A/N	42	12	R	Claimant's First Name
6	Date of Birth	N	54	8	R	Claimant's Date of Birth. Format is MMDDCCYY.
7	Sex Code	A/N	62	1	O	F =Female, M =Male, U =Unknown
8	State Agency Code	A/N	63	3	R	The 2-position State Code preceded by a 'U'. Format is Unn with nn being the SWA's State Code. Appendix C holds the State Codes.
9	Category of Assistance Code	A/N	66	1	R	Space

UIQ Response Record for SWAs not using offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
10	State Communication Code	A/N	67	3	R	Spaces
11	Welfare ID No.	N	70	22	R	Spaces
12	Date of WTPY Response	N	92	8	R	Date SSA responded. Format is MMDDCCYY.
13	Error Condition Code	N	100	3	R	Spaces = Input is valid, 101 =CAN invalid or missing, 102 =SSN invalid or missing; 103 =Both CAN & SSN invalid, 110 =CAN unverified, 120 =SSN unverified, 201 =Surname missing, 202 =Given name missing, 300 =DOB invalid, 400 =invalid sex code, 600 =Invalid query because inquired upon person is a public figure

UIQ Response Record for SWAs not using offset – cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
14	Identity Discrepancy Code	A/N	103	2	R	<p>Spaces=Match. If input query data does not match the identifying data on the queried record, the 2nd position of this field will be filled out.</p> <p>_2=Birthdate does not match on Title XVI record, _4=Given name does not match on Title XVI record, _6=Given name & birthdate do not match on Title XVI record,</p> <p>_8=Surname does not match on Title XVI record, _A=Surname & birthdate do not match on Title XVI record, _C=Surname & given name do not match on Title XVI record, _E=Surname, given name and birthdate do not match on Title XVI Match</p> <p>(if other codes received, ignore)</p>
15	Filler	A/N	105	3	R	Spaces

UIQ Response Record for SWAs not using offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
16	Verification Code	A/N	108	1	R	Indicates SSN verification or the reason for non-verification. V =SSN verified, X =SSN verified, records indicate individual is deceased, 1 =SSN not on file, 3 =Surname matched but DOB did not match, 5 =Surname does not match, F =SSN verified, surname ignored; M =SSN verified via MBR or SSR (overlay of '1'), P =SSN verified via MBR or SSR (overlay of '3'), R =SSN verified via MBR or SSR (overlay of '5'), Z =Verification code for record in which SWA submitted a CAN instead of an SSN. SSA found the CAN on the MBR, but did not verify the SSN. * =SSN not verified, & =Multiple SSNs are provided in the verified data field, up to 5.
17	Verification SSN Data	A/N	109	45	R	If Verification Code is *, this field contains the SSN located by SSA which differs from the SWA's SSN. If Verification Code is 3 or P, the DOB is contained. Format is MM/DD/CCYY If Verification Code is X, then date of death is contained. Format is MM/DD/CCYY If Verification Code is &, then multiple SSNs are contained.

UIQ Response Record for SWAs not using offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
18	Record Type	N	154	1	R	Indicates the content of the response 1 =Response is the standard response only 2 =Response contains Title II data
19	Title II Status	A/N	155	1	R	Indicates presence of a Title II record Y =Title II record exists, N =Title II record does not exist, C =SSA's Client Record Index indicates a record but it could not be located, D =SSA has a record but there's a name of DOB discrepancy between SSA's and the SWA's record, Space =SSA's Client Record Index is unable to obtain information as to the existence of a record or the request is for Prisoner data and CRI was not checked.
20	Title XVI Status	A/N	156	1	R	Indicates presence of a Title XVI record Y =Title XVI record exists, N =Title XVI record does not exist, C =SSA's index system was unable to find a record but there may be one, D =SSA has a record but the name or DOB on the SWA's is discrepant with SSA's information, Space =SSA's Client Record Index is unable to obtain information as to the existence of a record, or Prisoner data is requested and CRI was not checked.

UIQ Response Record for SWAs Using Offset

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
1	SSN	N	1	9	R	Social Security Number inquiring upon
2	CAN/BIC	A/N	10	12	O	Spaces
3	Surname	A/N	22	19	R	Claimant's Last name
4	Middle Initial	A/N	41	1	O	Claimant's Middle Initial
5	Given Name	A/N	42	12	R	Claimant's First Name
6	Date of Birth	N	54	8	R	Claimant's Date of Birth. Format is MMDDCCYY.
7	Sex Code	A/N	62	1	O	F =Female, M =Male, U =Unknown
8	State Agency Code	A/N	63	3	R	The 2-position State Code preceded by a 'U'. Format is Unn with nn being the SWA's State Code. Appendix C holds the State Codes.
9	Category of Assistance Code	A/N	66	1	R	Space

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
10	State Communication Code	A/N	67	3	R	Spaces
11	Welfare ID No.	N	70	22	R	Spaces
12	Date of WTPY Response	N	92	8	R	Date SSA responded. Format is MMDDCCYY.
13	Error Condition Code	N	100	3	R	Spaces = Input is valid, 101 =CAN invalid or missing, 102 =SSN invalid or missing; 103 =Both CAN & SSN invalid, 110 =CAN unverified, 120 =SSN unverified, 201 =Surname missing, 202 =Given name missing, 300 =DOB invalid, 400 =invalid sex code, 600 =Invalid query because inquired upon person is a public figure

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
14	Identity Discrepancy Code	A/N	103	2	R	<p>Spaces=Match. If input query data does not match the identifying data on the queried record, the 2nd position of this field will be filled out.</p> <p>2=Birthdate does not match on Title XVI record, 4=Given name does not match on Title XVI record, 6=Given name & birthdate do not match on Title XVI record,</p> <p>8=Surname does not match on Title XVI record, A=Surname & birthdate do not match on Title XVI record, C=Surname & given name do not match on Title XVI record, E=Surname, given name and birthdate do not match on Title XVI Match</p> <p>(if other codes received, ignore)</p>
15	Filler	A/N	105	3	R	Spaces

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
16	Verification Code	A/N	108	1	R	Indicates SSN verification or the reason for non-verification. V =SSN verified, X =SSN verified, records indicate individual is deceased, 1 =SSN not on file, 3 =Surname matched but DOB did not match, 5 =Surname does not match, F =SSN verified, surname ignored; M =SSN verified via MBR or SSR (overlay of '1'), P =SSN verified via MBR or SSR (overlay of '3'), R =SSN verified via MBR or SSR (overlay of '5'), Z =Verification code for record in which SWA submitted a CAN instead of an SSN. SSA found the CAN on the MBR, but did not verify the SSN. * =SSN not verified, & =Multiple SSNs are provided in the verified data field, up to 5.
17	Verification SSN Data	A/N	109	45	R	If Verification Code is *, this field contains the SSN located by SSA which differs from the SWA's SSN. If Verification Code is 3 or P, the DOB is contained. Format is MM/DD/CCYY If Verification Code is X, then date of death is contained. Format is MM/DD/CCYY If Verification Code is &, then multiple SSNs are contained.

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
18	Record Type	N	154	1	R	Indicates the content of the response 1=Response is the standard response only 2=Response contains Title II data
19	Title II Status	A/N	155	1	R	Indicates presence of a Title II record Y =Title II record exists, N =Title II record does not exist, C =SSA's Client Record Index indicates a record but it could not be located, D =SSA has a record but there's a name of DOB discrepancy between SSA's and the SWA's record, Space =SSA's Client Record Index is unable to obtain information as to the existence of a record or the request is for Prisoner data and CRI was not checked.
20	Title XVI Status	A/N	156	1	R	Indicates presence of a Title XVI record Y =Title XVI record exists, N =Title XVI record does not exist, C =SSA's index system was unable to find a record but there may be one, D =SSA has a record but the name or DOB on the SWA's is discrepant with SSA's information, Space =SSA's Client Record Index is unable to obtain information as to the existence of a record, or Prisoner data is requested and CRI was not checked.

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
21	Title II CAN/BIC	A/N	157	12	R	The Claim Account Number and Beneficiary Identification Code under which a Title II claim exists. The CAN portion of the claim number is the SSN of the wage earner on whose record benefits are being paid. See Appendix A for values.
22	State & County Code	A/N	169	5	R	SSCCC – where SS is the State Code and CCC is the county code from the Geographic Code Book that are responsible for any mandatory or optional supplementation payment.
23	Zip Code	N	174	5	R	The zip code of the residence address
24	Zip + 4	N	179	4	R	The additional 4 positions of the zip code
25	Number of Address Lines	N	183	1	R	The number of 22 position lines of address present
26	Address	A/N	184	132	R	6 address lines – each 22 bytes containing the residence address of the recipient.
27	Direct Deposit Indicator	A/N	316	1	R	Indicates if there is direct deposit data for benefits C =Checking S =Savings Space =None
28	Deferred Payment Date	N	317	6	R	Reflects the month and year the first or next payment can be made. Format is MMCCYY.

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
29	Schedule Payment Indicator	A/N	323	1	R	Indicates how the payments are made P =current month accrual amount paid by daily update operation R =current month accrual paid by monthly merge Space =prior month accrual only
30	Schedule Payment Date	N	324	6	R	Current operating month in which the Schedule Current Payment Amount was processed. (example, it would be 8/02 for a Schedule Current Payment that was paid in 9/02.)
31	Schedule Prior Payment Amount	N	330	7	R	Accumulated payment certified in the Schedule Payment action for all months through the Prior Month Accrual (PMA) date. Zeros are shown if no payment has been made. Amount is dollars and cents. Format is 9(4)v99.
32	Schedule Current Payment Amount	N	337	6	R	Amount certified in the Schedule Payment action for the current operating month as shown in the Schedule Payment Date. Amount is dollars and cents. Format is 9(4)v99.

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
33	Schedule Payment Combined Check Indicator	A/N	343	1	R	Y=combined check issued. Space=not applicable
34	LAF Code	A/N	344	2	R	Reflects the MBR payment status for this beneficiary. See Appendix A for values.
35	Date of Birth	N	346	8	R	Date of Birth. Format is MMDDCCYY.
36	Proof of Age Indicator	A/N	354	1	R	Indicates how age was proved. Values are: A =alleged, B =birth/baptismal, C =convincing evidence, F =formerly established by SSA, Q =established other than B or C
37	Given Name	A/N	355	10	R	Claimant's first name
38	Middle Initial	A/N	365	1	R	Claimant's middle initial
39	Surname	A/N	366	12	R	Claimant's last name
40	Date of Initial Entitlement	N	378	6	R	Date when beneficiary was originally entitled on this record. Format is MMCCYY.
41	Date of Current Entitlement	N	384	6	R	Date of entitlement to benefits for the current period of entitlement. Format is MMCCYY.

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
42	Date of Suspension or Termination	N	390	6	R	Date the event causing the suspension or termination occurred. Format is MMCCYY.
43	Sex Code	A/N	396	1	R	F =Female, M =Male, U =Unknown
44	Net Monthly Benefit if Payable (MBP)	N	397	6	R	Benefit payable after deduction of beneficiary obligations (like SMIB, overpayment, child support, etc). Amount is dollars and cents. Format is 9(4)v99.
45	Medicare Indicator	A/N	403	1	R	Indicates whether or not Medicare data is present Y =Medicare data is present N =Medicare data is not present
46	Health Insurance (HI) Indicator	A/N	404	1	R	Indicates whether or not Health Insurance is present. Y =Yes, N =No
47	HI Option Code	A/N	405	1	R	Health Insurance Option Code. C =None, cessation D =None, denied E =Yes, automatic F =None, invalid enrollment G =Yes, good cause H =None, not eligible or did not enroll P =Railroad, R =None-refused S =None, no longer under renal disease provision T =None, terminated for nonpayment of premiums W =None, withdrawal X =None-Title II termination Y =Premiums are payable

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
48	HI Start Date	N	406	6	R	Health Insurance Start Date. Format is MMCCYY.
49	HI Stop Date	N	412	6	R	Health Insurance Stop Date. Format is MMCCYY.
50	HI Premuim	N	418	5	R	Health Insurance premium amount collectible. Amount is dollars and cents. Format is S9(3)v99.
51	HI Buy-In Indicator	A/N	423	1	R	Indicates whether there is a third party code for health insurance Y=Yes, N=No
52	HI Buy-In Code	A/N	424	3	R	S01-S99 – indicates state billing T01-T99 – indicates third party billing
53	HI Buy-In Start Date	N	427	6	R	First month of coverage for which third party paid health insurance premium. Format is MMCCYY.
54	HI Buy-In Stop Date	N	433	6	R	Last month of coverage for which third party paid health insurance premium. Format is MMCCYY.

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
55	Supplemental Medical Insurance (SMI) Indicator	A/N	439	1	R	Indicates whether or not SMI data is present. Y = Yes, SMI Option Code contains Y, G, C, S, T or W N =No
56	SMI Option Code	A/N	440	1	R	Supplemental Medical Insurance Option Code. Values are Y =Yes, C =No, cessation, D =No, denied, F =No, terminated, G =Yes, good cause, N =No, no response, P =Railroad, R =no, refused S =No, no longer renal disease provision, W =No, withdrawal
57	SMI Start Date	N	441	6	R	Supplemental Medical Insurance first month of coverage. Format is MMCCYY.
58	SMI Stop Date	N	447	6	R	Supplemental Medical Insurance first month of non-coverage. Format is MMCCYY.
59	SMI Premium	N	453	5	R	Supplemental Medical Insurance premium amount collectible. Amount is dollars and cents. Format is S9(3)v99.
60	SMI Buy-In Indicator	A/N	458	1	R	Indicates whether there is a third party code for Supplemental Medical Insurance Y =Yes N =No
61	SMI Buy-In Code	A/N	459	3	R	Third Party Code for Supplemental Medical Insurance (Part B) A01-R99 =Third Party billing, 010-650 =State billing, 700 =Civil Service

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
62	SMI Buy-In Start Date	N	462	6	R	Effective Date of Supplemental Medical Insurance buy-in eligibility. Format is MMCCYY.
63	SMI Buy-In Stop Date	N	468	6	R	Date Supplemental Medical Insurance buy-in eligibility ended. Format is MMCCYY.
64	Welfare Agency Code	N	474	3	R	State exchange welfare code
65	Category of Assistance Code	A/N	477	1	R	State exchange categorical assistance code. A =Aged, B =Blind, C =AFDC, D =Disabled, F =Food Stamps, H =Health Maintenance, I =Income Maintenance, N =Title XIX Medicaid Eligibility, S =Statement of Consent
66	Black Lung Entitlement Code	A/N	478	1	R	Code concerning Black Lung Entitlement. D =Death Termination, E =Entitled, N =Nonpayment, P =Pending entitlement, T =Terminated (other than death)
67	Black Lung Payment Amount	N	479	6	R	Black Lung Payment Amount. Amount is dollars and cents. Format is 9(4)v99.
68	Railroad Indicator	A/N	485	1	R	A =Active Claim, T =Terminated Claim, S =Currently Suspended
69	Person's Own SSN	N	486	9	R	Person's Social Security Number

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
70	Date of Death	N	495	8	R	The date the person died. Format is MMDDCCYY.
71	Disability Onset Date	N	503	8	R	First date of onset of disability. Format is MMDDCCYY.
72	Number of Cross-reference Account Number (XRAN) Entries	N	511	1	R	The number of times the cross reference information (fields 73-75) contains valid data (up to 5)
						Note: Fields 73-75 occur 5 times
73	XREF Entitlement Number	A/N	512	9	R	If the Cross Reference Code= C , the first position of the Cross Reference Entitlement Number is an alpha code as follows: A =Beneficiary's own Civil Service Number, F =Beneficiary's survivor's Civil Service Number, S =Beneficiary's spouse's Civil Service Number. The last seven digits represent the Civil Service Number. If the Cross Reference Code is not a C, this field contains a social security number.
74	XREF BIC	A/N	521	2	R	The beneficiary identification code associated with the cross-reference entitlement number

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
75	XREF Code	A/N	523	1	R	Indicates what type of income the cross-reference number is.
76	Dual Entitlement Number	N	572	9	R	Other Claim Account Number on which entitlement exists
77	Dual Entitlement BIC	A/N	581	2	R	The beneficiary identification code associated with the dual entitlement number
78	Number of History Entries	N	583	2	R	The number of historical payment entries present on the response
						Note: Fields 79-81 occur 8 times Most recent information is in the 1 st occurrence
79	Monthly Benefit Credited (MBC) Date	N	585	6	R	Payment data credited date. MBC amount is paid in the month after this date. Format is MMCCYY.
80	MBC Amount	N	591	6	R	Monthly Title II benefit due after any appropriate dollar rounding but prior to the actual collection of any obligation of the beneficiary

UIQ Response Record for SWAs Using Offset - cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
81	MBC Type	A/N	597	1	R	C =Benefits paid, N =Benefits not paid, E =Benefits not paid, due to delayed/pending or suspense, Space =Benefits not paid
82	Other Date of Entitlement	N	689	6	R	The month and year of other date of entitlement. Format is MMCCYY.
83	Other Primary Insurance Amount	N	695	6	R	The controlling primary insurance amount (PIA) for payment on the other claim, whether average month wage or special minimum. Amount is dollars and cents. Format is 9(4)v99.
84	Other Retirement Insurance Amount	N	701	6	R	Appears only if the controlling primary insurance amount (PIA) reflects the average monthly wage PIA for the other claim. Amount is dollars and cents. Format is 9(4)v99.
85	Larger Full Monthly Benefit Amount	N	707	6	R	Larger full monthly benefit amount (LFMBA) reduced for the family maximum. In the case of triple entitlement, LFMBA in the first dual entitlement field for the auxiliary (B) claim, and LFMBA in the second dual entitlement field is for the survivor (D) claim. Amount is dollars and cents. Format is 9(4)v99.

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
86	Larger Excess Monthly Benefit Amount	N	713	6	R	Excess amount payable on the larger excess monthly benefit amount (LEMBA). In the case of triple entitlement, LEMBA in the first dual entitlement field is for the auxiliary (B) claim, and LEMBA in the second dual entitlement field is for the survivor (D) claim. Amount is dollars and cents. Format is 9(4)v99.
87	Smaller Full Monthly Benefit Amount	N	719	6	R	Smaller full monthly benefit amount (SFMBBA) reduced for family maximum. In the case of triple entitlement, SFMBBA in the first dual entitlement field is for the primary (A) claim, and SFMBBA in the second dual entitlement field is blank. Amount is dollars and cents. Format is 9(4)v99.
88	Smaller Actuarially Reduced Monthly Benefit Amount	N	725	6	R	The smaller monthly benefit amount reduced for maximum and age (SAMBA). Amount is dollars and cents. Format is 9(4)v99.

UIQ Response Record for SWAs Using Offset- cont.

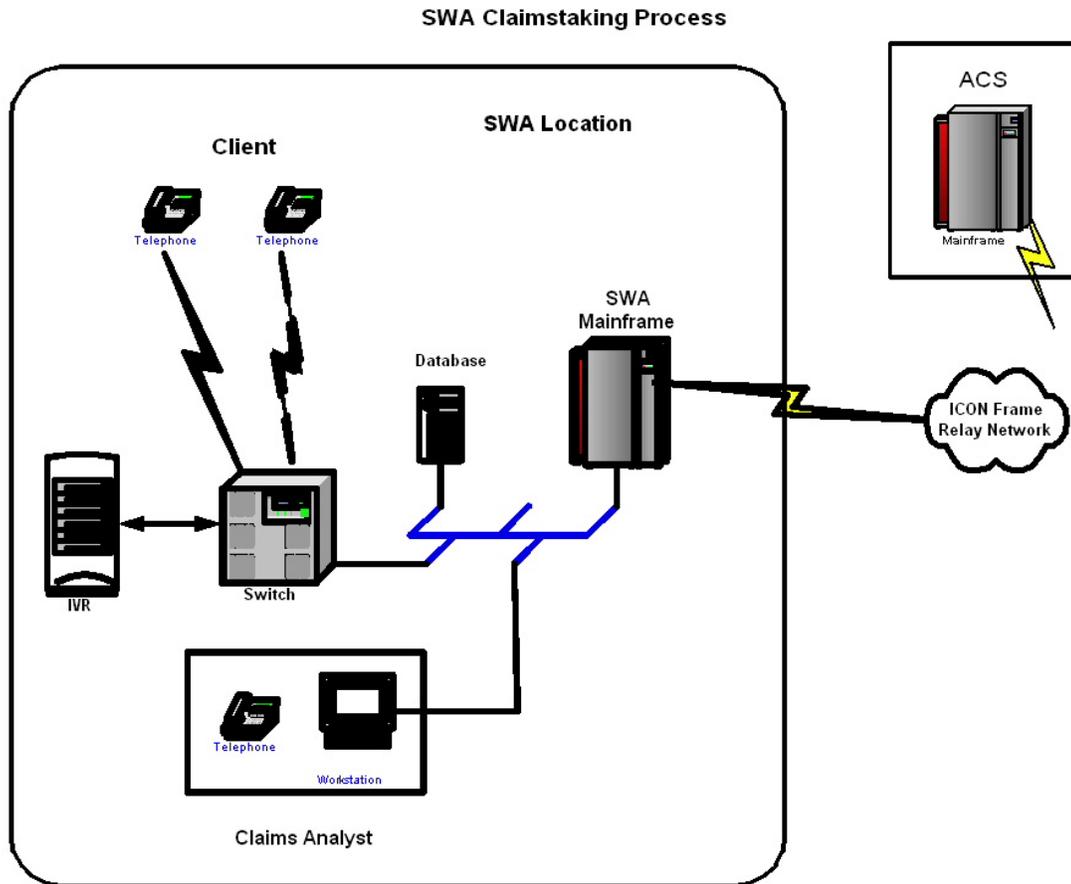
FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
89	Dual Entitlement Status Code	A/N	731	1	R	For triple entitlement cases, dual entitlement status code is based on the primary (A) and auxiliary (B) claims. It is assumed that the survivor (D) benefit is in the payment status as the primary payment status. Values are: Space =Default value, 0 =Neither benefit in current payment status, 1 =smaller benefit only in current payment status, 2 =Larger benefit only in current payment status, 3 =Both benefits eligible for current payment status (checks may be combined or separate), 4 =Primary is working on record on which auxiliary entitlement exists, 5 =Larger benefit is subject to full government pension/worker's compensation offset, S =Dual entitlement suspended, technical entitlement exists, T =Dual entitlement terminated
90	Other Office Code	N	732	1	R	1-8 =Payment center that has jurisdiction A-H =Payment center that has jurisdiction when wage earner is disabled.
91	Type of Dual Entitlement	A/N	733	1	R	Type of dual entitlement on the MBR. 1 =Primary/Auxiliary (or Survivor), 2 =Survivor/Auxiliary, 3 =Insured/Prouty, 4 =Triple entitlement

UIQ Response Record for SWAs Using Offset- cont.

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
92	Other Primary Insurance Amount Factor Code	A/N	734	1	R	Equals the primary insurance factor code values in the other account. A =Special Age 72 (Prouty) – Transitionally insured (as of 6/82 or later), B =Average monthly wage, C =Special minimum, E =Death primary insurance amount (PIA) average monthly wage, F =Death PIA special minimum, G =AMW life and death special minimum, PIAs are equal, K =Prorated (totalized) PIA, L =Average indexed monthly earnings, M =Minimum PIA if greater than average indexed monthly earnings (AIME), N =New start guarantee PIA, O =Old start guarantee PIA, S =Subsequent disability insurance benefits (DIB) guarantee PIA, V =Modified old start windfall PIA, Z =Northern Mariana Islands (NMI) computation (for future use), 5 =Modified new start windfall PIA, 7 =1990 new start, 8 =1990 old start
93	Other Primary Insurance Amount Factor Code Two	A/N	735	1	R	For future use – the primary insurance factor code 2 in the other account
94	Other Eligibility Year	N	736	4	R	The other eligibility year. Format is CCYY.

9.0 SWA Claimstaking Diagram

Below is a diagram of an SWA's initial claimstaking process. It is in this process that the software hook to send a UIQ request and process a UIQ response will be placed.



10.0 Impact to SWA

In order for your state to participate in the data exchange with the SSA, your action items will be as follows:

SWA will sign agreement with SSA.

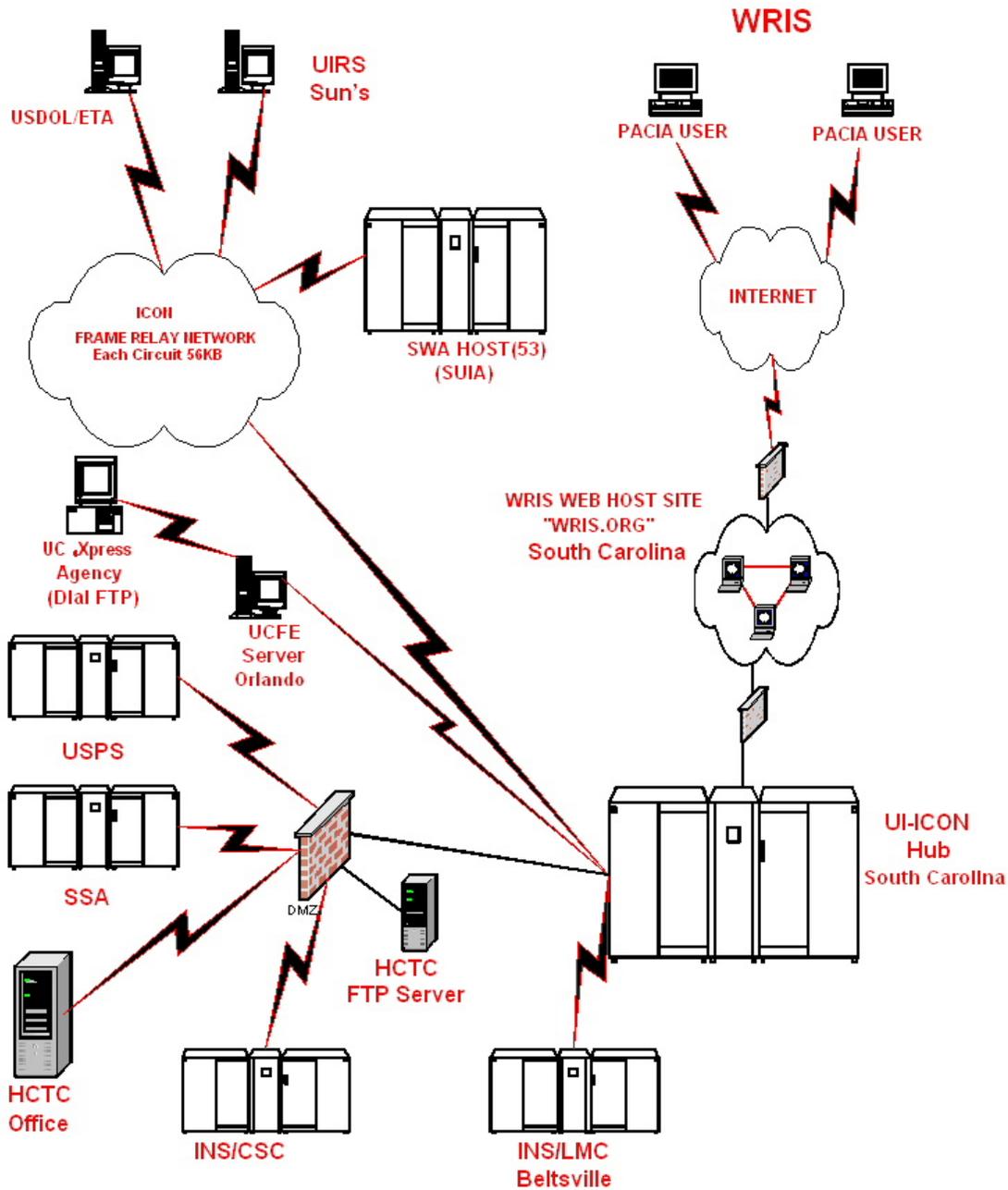
Allow SSA access to SWA's IBIQ. To do this if you have the IBIQ model code, add 'SS' as a valid code in the working storage section of program INPOIQ00, in the 88 level called 'WS-VALID-CODE', and recompile the program.

Send SSA UIQ requests and process responses. Incorporate the sending and receiving of the UIQ data into your initial claims process.

11.0 ICON Network Diagram

With the addition of the UIQ application, the ICON expanded network is reflected below.

Current UI - ICON Network



12.0 TCP/IP SWAs

States that communicate via TCP/IP will need to add an 8 byte TCP/IP header on the front of their requests. The TCP/IP header contains the transaction code and total number of bytes sent. A request is coded **'UIQT0138'**.

UIQ TCP/IP Header

FLD NBR	FIELD NAME	FIELD TYPE	BEGIN COLUMN	FIELD LENGTH	REQ/OPT	DESCRIPTION
1	TCPIP-TRANSACTION	A/N	1	4	R	Transaction code to send to the hub - UIQT
2	TCPIP-NBR-OF-BYTES	N	5	4	R	Total number of bytes sent – 0138 for UIQ requests

Appendix A

LAF Code

A	Withdrawal for adjustment
AA	Adjusted to split PICs in Advance File Status
AC	PIA correction
AD	Adjusted for dual entitlement
AE	Withdrawn for recomputation under Section 142 (Japanese Internment credits)
AF	Transferred to another program service center or OIO
AJ	Worker's compensation offset/ public disability benefits cancellation
AM	Withdrawn from HIB-only status
AP	Withdrawn for change of PIC or postentitlement action
AR	Withdrawal of a beneficiary from LAF S or T to place in current payment status
AW	Withdrawn to impose worker's compensation offset/public disability benefits
A&	Withdrawn from suspense or deferred status to be placed in current payment status
A-	Withdrawn from current payment status to be placed in suspense or deferred status
AO	Withdrawn to adjust reduction factor
A1	Withdrawn for recomputation under Section 229
A2	Withdrawn for 1965 or 1968 recomputation

A3	Withdrawn for recomputation under Sections 217 and 229
A4	Withdrawn for disability offset recomputation
A5	Withdrawn for recomputation not separately defined
A6	Withdrawn to recalculate PIA to include disability freeze
A7	Withdrawn for recomputation under Section 217
A8	Record transferred from OIO to another program service center
A9	Withdrawn for adjustment action not separately defined
B	Abatement status
C	Current payment status (except railroad payment)
D	Deferred payment status
DP	Deferred because of Public Assistance
DW	Deferred for Worker's Compensation/public disability benefit offset
D1	Deferred for Foreign work test
D2	Deferred for annual retirement test
D3	Deferred as an auxiliary because the primary beneficiary is LAF-D2
D4	Deferred for no child-in-care
D5	Deferred as an auxiliary because the primary beneficiary is in LAF-D1
D6	Deferred to recover overpayments not separately defined
D9	Deferred for reasons not separately defined

E	Current payment certified to the Railroad Retirement Board (RRB)
N	Disallowed claim
ND	Denied claim
P	Delayed claim (adjudication pending)
PB	Delayed claim - beneficiary's claim not finally adjudicated
PT	Claim has been terminated from delayed claims status
R	Kill Credit
Sx	Conditional status
SB	Benefits due but not paid (less than \$1.00)
SD	Technical entitlement—either the beneficiary is entitled on another claim, or the disability family maximum provision has reduced the MBA to zero
SF	Prouty beneficiary fails to meet residency requirement
SH	Prouty beneficiary receiving government pension
SJ	Alien suspension
SK	Suspended because of deportation
SL	Suspended because the beneficiary is in a barred payment country
SP	Suspended because Prouty beneficiary receiving public assistance
SS	Nonpayment to post secondary students during summer months
SW	Worker's compensation/public disability benefit offset
S0	Suspended determination of continuing disability is pending

S1	Suspended because worked outside the United States (U.S.)
S2	Suspended because beneficiary worked inside the U.S.
S3	Suspended because the primary beneficiary worked in the U.S.
S4	Suspended for failure to have child-in-care
S5	Suspended because primary beneficiary worked outside the U.S.
S6	Suspended during development of a better (correct) address for mail or direct deposit, as appropriate
S7	Prisoner suspension, suspension due to extended trial work period (EPE SGA); or suspension for refusing vocational rehabilitation (VR) services.
S8	Suspended while payee is being determined
S9	Miscellaneous suspension
Tx	Terminated status
TA	Advance filing claim terminated before maturity
TB	Mother, Father terminated-entitled to disabled widow(er)s benefits
TC	Disabled widow attained age 62 and is not entitled as an aged widow
TJ	Advance filed claim terminated after maturity
TL	Termination of post-secondary student
TP	Terminated for change of payment identification code (PIC) on postentitlement actions
T&	Claim was withdrawn

T-	Disability benefits terminated because of conversion to retirement benefits upon attainment of age 65
T0	Benefits payable by some other agency
T1	Death of beneficiary
T2	Dependent terminated due to death of primary beneficiary
T3	Divorce, marriage, remarriage
T4	Attainment of age 18 or 19 and not disabled; mother/father terminated based on last child's attainment of age 16
T5	Entitled to other benefits
T6	Child beneficiary is no longer attending school on full-time basis and is between ages 18 and 19, or a disabled child is no longer under a disability. Termination of a mother because of death or marriage of the last remaining child entitled to receive benefits
T7	Adoption of child; mother terminated, last entitled child adopted
T8	Primary DIB no longer disabled; mother/ father terminated, child no longer disabled
T9	Terminated for reasons not separately defined
U	Active uninsured status
W	Withdrawal before entitlement
Xx	Adjusted/Suspended/Terminated/ Un-insured status
XD	Withdrawal for adjustment
XF	Entitlement transferred to another program service center or OIO

XK	Beneficiary deported
X+	SMI withdrawn; beneficiary entitled only to SMI
X0	Claim transferred to RRB
X1	Death of beneficiary
X5	Entitled to other benefits
X7	Health insurance benefits (HIB)/ SMIB terminated
X8	Payee being developed
X9	Entitlement has been interrupted for reasons not separately defined

Appendix B

UIQ ERROR MESSAGES

SERVER (QV00C00)

E400	INVALID COMMAREA LENGTH
E420	INVALID APPLID REQUEST (currently A = SOLQ, only valid id so far)
E440	NO VALID SSN OR CAN RECEIVED (ssn/can is spaces or not numeric)
E888	INVALID DATE OF BIRTH (see QV02C00 error list)
S400	ERROR GETTING MEMORY (error on GETMAIN)
S401	FAILED – TERMERR (terminal error)
S402	FAILED – LENGERR (length exceeds the max)
S403	FAILED – NOTALLOC (facility specified not owned by the application)
S404	FAILED – NOTALLOC (issued for any other non-zero return code)
S425	BAD LINK TO SOLQ APPL (bad link to driver QV02C00)
S430	BAD LINK TO GU02 (gu02c00)
S435	BAD RETURN FROM GU02 (gu02c00)

DRIVER (QV02C00)

E101	SSN INVALID (input ssn is spaces)
E102	SSN INVALID (input ssn is not spaces)
E110	EVS FAIL (input ssn is spaces)
E120	EVS FAIL (input ssn is not spaces)
E600	(from IENP) BAD RETURN FROM IENP
E710	CRI-FAIL
E888	(Field edits)
	- INVALID SOC. SEC. NUMBER
	- INVALID STATE CODE
	- INVALID DATE OF BIRTH (in QV00C00 – not in QV02)
	- INVALID SIRNAME
	- INVALID GIVEN NAME
	- NON NUMERIC BENE PAY NUMBER (ric x ssn is nonnumeric)

S505 (Multiple messages returned from GUNUC00)

- ERROR LINKING TO GUNUC01
- FNAV** - ERROR NUMIDENT NOT AVAILABLE
- GCTP** - ERROR LINK TO GCTPCELP FAILED
- GTM1** - ERROR GETMAIN FOR DEC FAILED
- GTM2** - ERROR GETMAIN FOR COMPRESSED FAILED
- GUDB** - ERROR LINK TO GUNMC00 FAILED VERIFY DOB
- GUNM** - ERROR LINK TO GUNMC00 FAILED VERIFY NAME
- LNGE** - ERROR WRONG COMM-AREA LENGTH PASSED TO GUNUC00
- RNIF** - ERROR RECORD NOT IN FILE

(from CRIGET)

- BAD RET CRI-ST
- ERROR LINKING TO CRI PROGRAM EQ04C00
- ERROR CRI TABLE FULL
- BAD RETURN FROM CRIGET (cri return is not 12 or **** or RNIF)
- RT12** - CRI RETURN CODE IS 12

(from IENP)

- ERROR LINKING TO IENPVAL

(Others)

- ERROR LINKING TO PROGRAM QV03C00
- ERROR LINKING TO CRI PROGRAM EQ04C00
- ERROR LINKING TO MBR PROGRAM EQ01C00 (MBR read)
- ERROR IN GETMAIN FOR SSR
- ERROR GETTING MEMORY (GETMAIN)

SUB-SUPR (QV03C00)

- S502** PROBLEM BRKDWN-SPREAD
- S503** PROBLEM SSR-SPREAD
- S505** ERROR LINKING TO PROGRAM QV04C00
- S505** ERROR LINKING TO PROGRAM QV05C00

Appendix C

These are the State Codes used by SSA:

Alabama	01	Nebraska	28
Alaska	02	Nevada	29
Arizona	03	New Hampshire	30
Arkansas	04	New Jersey	31
California	05	New Mexico	32
Colorado	06	New York	33
Connecticut	07	North Carolina	34
Delaware	08	North Dakota	35
Dist of Columbia	09	Ohio	36
Florida	10	Oklahoma	37
Georgia	11	Oregon	38
Hawaii	12	Pennsylvania	39
Idaho	13	Puerto Rico	40
Illinois	14	Rhode Island	41
Indiana	15	South Carolina	42
Iowa	16	South Dakota	43
Kansas	17	Tennessee	44
Kentucky	18	Texas	45
Louisiana	19	Utah	46
Maine	20	Vermont	47
Maryland	21	Virgin Islands	48
Massachusetts	22	Virginia	49
Michigan	23	Washington	50
Minnesota	24	West Virginia	51
Mississippi	25	Wisconsin	52
Missouri	26	Wyoming	53
Montana	27		

Glossary

ACS	Affiliated Computer Services, Inc.
DOL	Department of Labor
PLD	Program Logic Document
IBIQ	Interstate Benefits InQuiry
ICON	Interstate Connection
IVR	Interactive Voice Response
SOLQ	State On Line Query
SSA	Social Security Administration
SWA	State Workforce Agency
UI	Unemployment Insurance
UIQ	Unemployment Insurance Query

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

3/17/2004

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.

C. 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.

**SWA Access to SSA Data
through the Interstate Connection Network
IV&V Specifications**

3/17/2004

Table of Contents

1.0 Purpose.....	1
2.0 Background	1
3.0 SWA System Security Certification Review.....	1
3.1 <i>Review of System Design Documentation.....</i>	2
3.2 <i>Automated Audit Trail</i>	2
3.3 <i>System Access Control.....</i>	3
3.4 <i>Monitoring and Anomaly Detection</i>	4
3.5 <i>Management Oversight and Quality Assurance</i>	5
3.6 <i>Security Awareness and Employee Sanctions.....</i>	5
3.7 <i>After certification and Periodic Certification Review(s).....</i>	5
4.0 SWA Certification submission to DOL.....	6
4.1 <i>Initial Determination</i>	6
4.2 <i>Final Determination</i>	6
APPENDIX A	7

SWA Access to SSA Data Through the Interstate Connection Network IV&V Specifications

1.0 Purpose

The purpose of this document is to describe the requirements for verifying SWA compliance with the Social Security Administration's systems security requirements for connecting to SSA's Unemployment Insurance Query program through the ICON. Each SWA that implements the online connection to SSA through ICON must have an independent certification performed by a professional auditor that offers Independent Verification and Validation (IV&V) services. SWA's must obtain this systems security compliance certification prior to being authorized by DOL to access SSA information through the ICON. Additionally, a DOL official will use this document, as a guide, when evaluating and certifying the SWAs' system design.

SWAs must first negotiate a data sharing agreement with SSA before a systems security certification and compliance review can be conducted by an IV&V contractor. Following initial systems security compliance certification through this process, SSA will monitor ongoing SWA compliance with their systems security requirements through its own periodic onsite reviews.

2.0 Background

SSA is required by law to protect personal information from unauthorized use or disclosure. The Director, SSA Office of Systems Security Operations Management is responsible for assuring that external systems that receive information from SSA are secure and operate in a manner that is consistent with SSA's own systems security policies, and are in compliance with the terms of information sharing agreements executed by SSA. Normally, in carrying out this responsibility, SSA requires data exchange partners who request online access to submit written documentation of their system design and security features, and then SSA conducts onsite verification prior to allowing the exchange partner to access information from SSA. For the purpose of facilitating SWA access to SSA information through the ICON, DOL has agreed to take on this responsibility and certify that SWA's have complied with SSA's systems requirements.

3.0 SWA System Security Certification Review

Each state must have a systems security certification review completed by an independent third-party and be "certified" as meeting the SSA security requirements before they can connect to SSA's UIQ program through ICON. The reviewer must be a qualified vendor or accredited auditor offering IV&V services for information systems including technological systems security applications and procedures.

The required systems security certification review will consist of an onsite inspection of the SWA's client support system and data center to observe physical security safeguards, a demonstration of the implementation of the UIQ connectivity to the SSA information, and discussion of each of these requirements with the SWA's responsible management personnel. The reviewer also will request a demonstration of the SWA's audit trail capability and will visit at least one of the SWA's field offices to review the SWA's implementation of systems security awareness procedures and procedures regarding the proper handling and protection of SSA-supplied information with workers and managers.

The following section describes the steps that must be performed in order to certify that the SWA meets the SSA systems security requirements for online access, as specified above in section 3.

Note: All references to written documentation can be taken to mean either hardcopy or online documentation, unless specified otherwise. Where written signatures are required, document imaging systems may be used to retain copies of signed documents, or digital signatures may be employed where authorized by state law or Federal laws where applicable.)

3.1 Review of System Design Documentation

The IV&V contractor will verify that the SWA has submitted to DOL written systems security documentation conforming to SSA requirements. DOL will provide a copy of this documentation to the contractor in advance of the scheduled onsite review of the SWA.

The SWA documentation that the IV&V contractor will use as the basis for their verification and validation review will consist of the documentation specified in the Systems Security Requirements for SWA Access to SSA Information Through the ICON System which is attached to the individual data exchange agreements between SWA's and SSA. A copy of this document also is attached to this document at Appendix A.

The IV&V contractor will verify and certify in their report that the SWA's system design documentation addresses each of the SSA system security requirements as specified in SSA's requirements document.

3.2 Automated Audit Trail

- The IV&V contractor will verify and certify in their report that the SWA has an audit trail system
- The reviewer, with the assistance of SWA personnel, will verify that the audit trail capability conforms to SSA requirements, and is able to:
 - a. Identify the SWA employee who initiated the online query request for SSA information, or the SWA client case associated with the transaction if the query is systems generated.

- b. Identify the time and date of the request, as well as
- c. Identify the client case related to the transaction.

3.3 System Access Control

- The IV&V contractor will verify and certify in their report that the SWA's system access control process and infrastructure conforms to SSA requirements. The reviewer will meet with the individual(s) responsible for System Access Control functions and observe a demonstration of the procedures for logging onto the system for accessing SSA information through the online query.
- The reviewer will verify that a written description of the SWA's Data Exchange technological access controls has been created. The document must:
 - a. Identify the type of software used. If commercial packages are employed, or authentication/access control features of common operating systems are used (e.g., Windows or UNIX user accounts coupled with various types of group access), the version and maintenance level should be documented. If custom software is specified, identify the developer or vendor and provide the user documentation for review.
 - b. Provide an overview of the process used to grant access to protected information for workers in different job categories, and
 - c. Provide a written description of the function responsible for PIN/password issuance and maintenance.
- The reviewer will verify that the SWA's system access control uses a recognized user access security software package (e.g. RAC-F, ACF-2, and TOP SECRET) or an equivalent security software design. Where access to a mainframe is required as part of the UIQ, verification will include a demonstration of RACF authentication/authorization using a valid password, as well as demonstration of logon failure when incorrect passwords are provided.
- The reviewer will verify that the access control software utilizes personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. System verification will include a demonstration showing that two-factor authentication (e.g., PIN/Password or PIN/Biometric identifier) allows access the UIQ system, as well as demonstrating that invalid credentials will cause logon failure.
- The reviewer will verify that the SWA has management controls and oversight of the function of issuing and maintaining access control PINs and passwords ensuring only authorized users have access to UIQ. Verification will consist of reviewing the written procedures that cover the process.

3.4 Monitoring and Anomaly Detection

- The reviewer will verify that the SWA’s system design for online access to SSA information includes monitoring and anomaly detection capabilities to deter employees from browsing unauthorized information.

An illegal access, “accessing SSA records not associated with a UI claim”, will be attempted and verification will determine whether appropriate actions are initiated by the system (i.e., logging, access denial).

- The reviewer will verify that the SWA’s system design can produce reports indicating the capability to appropriately monitor user access. Legal and illegal accesses will be performed and the ensuing reports will be examined for expected results.
- The reviewer will review the reports for content appropriateness based upon the report type, such as:

a. 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, including failed attempts to enter a password.

b. Inquiry match exception reports

This type of report captures information about users who may be initiating UIQ transactions for Social Security Numbers that have no client case association within the outside entity’s system.

c. System error exception reports

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

d. Inquiry activity statistical reports

This type of report captures information about UIQ usage patterns among authorized users.

- The reviewer will also meet with SWA employees responsible for reviewing such reports. Documented procedures for reviewing both standard and exception reports will be examined, individual responsible for conducting the review will be identified and documented methods for tracking problems identified by reports will be reviewed.
- The reviewer will certify that the SWA has anomaly detection procedures for the SWA’s employees responsible for reviewing the reports, addressed above. Anomaly reports will be reviewed for ease of use. Written procedures for distributing reports

and assigning responsibility will be reviewed. If anomalies are buried in general log files, methods employed to facilitate exception handling will be demonstrated by the reviewers to verify that anomalies can be readily identified.

3.5 Management Oversight and Quality Assurance

- The reviewer will verify that the SWA has established ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information. Verification will include the review of documented procedures, as well as a review of a log or other method used to control issuance of access to the UIQ system.
- When certifying the SWA's system, SSA will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out.

3.6 Security Awareness and Employee Sanctions

- The reviewer will verify that the SWA is providing security awareness training for employees. Verification will include documented training schedules or procedures. The period examined will include the previous year and plans for the following year. Records that are used to verify that employees have received appropriate training will be examined.
- The reviewer will verify that the security awareness training provided includes information about the SWA's responsibility for:
 - a. Proper use
 - b. Proper protection of SSA information, and
 - c. Possible sanctions for misuse of online access to SSA information.

Verification will include a review of the training materials.

- The reviewer will obtain information on how these functions will be performed within the SWA's organization, identifying the individual(s) or component(s) responsible for performing the functions. Verification will determine that an individual or the department has been assigned responsibility for the training, and that training has been conducted in accordance with a documented plan.
- Additionally, the reviewer will meet with the individuals responsible for these functions and request a written description of how these responsibilities are carried out.

3.7 After certification and Periodic Certification Review(s)

- After certification and upon network connectivity to the SSA UIQ, the reviewer will perform a follow-up certification review after live transmission of SSA online information to the SWA. The reviewer will verify the automated audit trail capability by asking the SWA to retrieve audit trail information for a sample of live transactions received by SSA. The information submitted to the reviewer, in support of the sample transactions, must be certified as accurate by an appropriate management official of the SWA.

4.0 SWA Certification submission to DOL

Generally, the certification review will address each of the requirements described above and will include, where appropriate, a demonstration report of the SWA's implementation of each requirement. The reviewer must certify that the SWA system design for online access to SSA information includes all security elements as required by SSA.

4.1 Initial Determination

- Following a successful security certification review, the reviewer will submit an initial determination certification report to DOL as well as the SWA.
- DOL will have 21 working days to respond to the initial determination certification review report.

4.2 Final Determination

- The reviewer will address each comment of the initial determination and submit a final determination certification report to DOL.

No specific format for submitting this information is required. However, regardless of how it is presented, the initial determination and final determination document should be submitted covering each of the items in section 3.0, above, over the signature of an official representative of the SWA.

APPENDIX A

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.

C. 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.

Regional Office Online Data Exchange Coordinators

Region	Coordinator	Telephone Number	Fax Number	Email Address
Boston	Alan Hobbs	617-565-2887	617-565-9359	alan.hobbs@ssa.gov
New York	Dan Karp Bob Ievers	212-264-1065 607-733-4206	212-264-5257 607-734-6829	Dan.Karp@ssa.gov Bob.Ievers@ssa.gov
Philadelphia	John Bielski Maryann T. Thomas	215-597-0738 215-597-2486	215-597-7271 215-597-7271	john.bielski@ssa.gov Maryann.T.Thomas@ssa.gov
Atlanta	Don E. Hatcher Steve Roberts Herbert H. Vaughan	205-801-1801 205-801-1809 205-801-1808	205-801-1804 205-801-1804 205-801-1804	don.hatcher@ssa.gov steve.roberts@ssa.gov herbert.h.vaughan@ssa.gov
Chicago	John H. Williams	312-575-4015	312-575-4245	John.H.Williams@ssa.gov
Dallas	Karen Palmer	214-767-4304	214-767-1348	karen.palmer@ssa.gov
Kansas City	Leah Ann McCormick	816-936-5650	816-936-5951	leah.ann.mccormick@ssa.gov
Denver	Dave Mellinger	303-844-4260	303-844-3281	dave.mellinger@ssa.gov
San Francisco	Ellery Brown	510-970-8243	510-970-8101	ellery.brown@ssa.gov
Seattle	Kate Pesin	206-615-2130	206-615-2643	kate.pesin@ssa.gov

10/31/03

To: Regional Office / DOL Regional Director for UI
From: Steve Miksell / Security Programs / ITSC
Subject: SSA Integrity Cross Match

12 March 2004

A formal agreement to allow UI agencies to access Social Security data on-line via the Unemployment Insurance Query (UIQ) has been finalized. The intent of this cross matching of information is the enhancement of the integrity of the Initial Claims process. One of the conditions that must be satisfied prior to access being granted is an independent review of the Initial Claims deployment where the SSA access will occur. The Information Technology Support Center has developed an Independent Verification approach designed to satisfy this requirement. If you are aware of states in your region that may require this service, please make them aware of this capability. If there are further questions about this support capability please feel free to contact the ITSC, or direct inquiries to our attention.

I can be contacted at:

Steven Miksell, D.Sc., CISSP
9658 Baltimore Avenue #400
College Park, MD
20740
Telephone (301) 982-1116
Email: smiksell@itsc.org

Additional Contact at same location:

Jane Powanda, Senior Security Specialist
Telephone (301) 513-0143
Email: jpowanda@itsc.org

Regards, Steve Miksell