

1.0 BACKGROUND OF THE FEDERAL PARENT LOCATOR SERVICE

The Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA) of 1996 mandates the establishment of new resources at the Federal and State levels to assist state Child Support Enforcement (IV-D) agencies in:

- establishing paternity;
- establishing, setting the amount of, or modifying child support obligations; and
- enforcing child support obligations.

Some of the provisions of PRWORA require the establishment of State Directories of New Hires (SDNH), State Case Registries (SCR), and, within a Federal Parent Locator Service (FPLS), a National Directory of New Hires (NDNH), and a Federal Case Registry of Child Support Orders (FCR). The implementation date for the NDNH is October 1, 1997 and October 1, 1998 for the FCR.

A state's SDNH is a registry of all newly hired employees in that state and the SCR is a registry of all the state's IV-D child support cases and all support orders established or modified in the state on or after October 1, 1998. Each SDNH and SCR transmits data to the NDNH and the FCR components of the FPLS respectively. In addition, each state also transmits quarterly wage and unemployment insurance data to the NDNH.

In order to have a comprehensive database with information from all employers, PRWORA also requires every Federal agency to transmit information on newly hired employees and quarterly wage information to the NDNH. Federal agencies transmit their data directly to the NDNH.

1.1 Purpose of the National Directory of New Hires

The purpose of the NDNH is to provide a national repository of employment and unemployment insurance information that will enable state IV-D agencies to be more effective in locating non-custodial parents, establishing child support orders and enforcing child support orders. The information in the NDNH, as a part of the FPLS, alleviates many of the difficult issues inherent in interstate child support enforcement.

Custodial Parties, Non-custodial Parents and Putative Fathers in IV-D child support cases, as reported by the SCRs, are compared with the quarterly wage (QW), unemployment insurance (UI) and new hire (W-4) data that the Federal agencies and states submit. Any matching information is made available to the state IV-D agencies. This information, combined with other available locate and enforcement remedies, enables the agencies to be more effective in enforcing and collecting child support.

In addition to the information accessible to state IV-D agencies, NDNH data may be accessed by the following authorized users:

1. the Internal Revenue Service (IRS),
2. the Social Security Administration (SSA),
3. authorized persons investigating parental kidnapping,
4. persons authorized to obtain information to locate a parent or child for the purpose of making or enforcing child custody and child visitation determinations,
5. state IV-B and IV-E agencies in order to locate persons for the purposes of adoption,
6. the Department of Education (DoEd),
7. the Department of Housing and Urban Development (HUD),
8. state IV-A agencies for IV-A program purposes, and
9. State Workforce Agencies (SWA).

1.2 System Functionality

Figure 1-1 is a representation of NDNH functionality. This diagram shows the types of information that flow into and out of the system. The following is a description of the processing of NDNH information for each agency shown on the diagram.

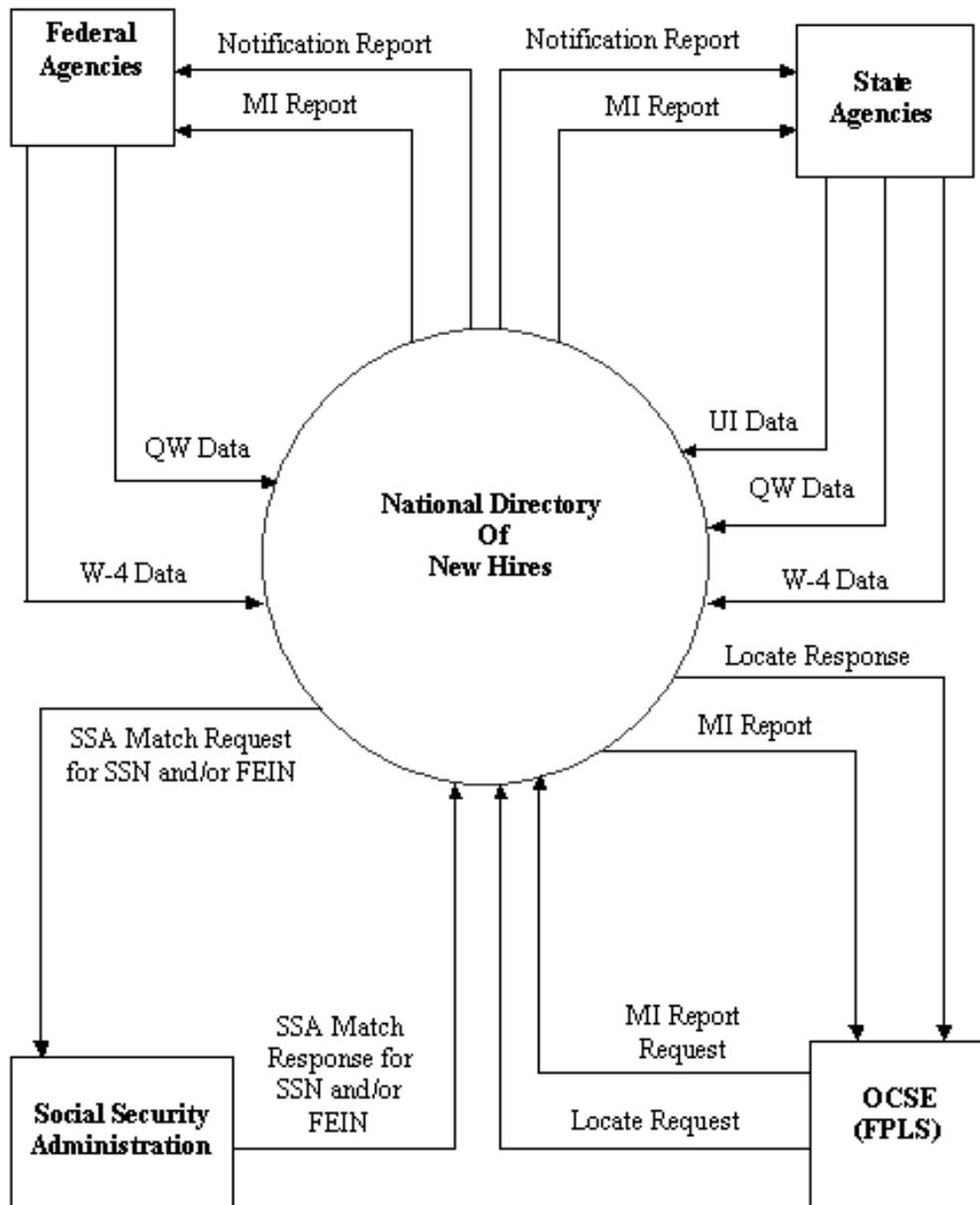
Federal Agencies – Each Federal agency or its payroll department submits W-4 and QW data directly to the NDNH for processing and inclusion on the NDNH database. Each Federal submitter receives a Notification Report providing information about the submitted data, such as the total number of W-4 or QW records received, processed data errors, and SSN verification information. They also receive a regularly scheduled Management Information (MI) report to assist in the monitoring of W-4 and QW reporting.

State Agencies – There are various state agencies that receive and transmit W-4, QW and UI data to the NDNH. They include SDNHs in Child Support Enforcement IV-D agencies, State Workforce Agencies (SWAs), State Departments of Revenue, and any other agency a state may designate as the responsible agency for receiving and transmitting the W-4, QW or UI data. Each submitting state agency receives a Notification Report providing information about the submitted data, such as the total number of records received and processed by the NDNH, data errors, and SSN verification information. They also receive a regularly scheduled MI report to assist in the monitoring of data reporting.

Social Security Administration – When the NDNH receives a record containing an SSN and name, the NDNH transmits the data to SSA, which attempts to verify the SSN by matching the information against SSA records. The NDNH records the results of SSN verification attempts. In addition, when the NDNH receives a record containing a Federal Employer Identification Number (FEIN), but not an employer address, system processing attempts to match the FEIN against SSA's Employer Identification File (EIF) to obtain the employer's address.

OCSE – OCSE automatically receives regularly scheduled MI reports to assist in the monitoring of the NDNH System and State and Federal agency compliance. In addition, the NDNH receives requests for locate information on individuals through the FPLS. The NDNH System receives a Locate Request, attempts to match the incoming record to W-4, QW and UI data, and reports matches back to the FPLS, which then reports the information to the requesting agency.

Figure 1-1: NDNH Functionality Diagram



2.0 SECURITY

Security and privacy are crucial and integral components, which have been, and will continue to be, considered throughout the development and operation of the Federal Parent Locator Service.

2.1 Controlling Authority for Security Legislation

Various applicable statutes, OMB Bulletins, FIPS Publications and HHS policies establish specific requirements for confidentiality, integrity and availability of information in the FPLS and address and provide guidance on these issues. Safeguards that support these legislative acts are in place to ensure the accuracy of the FPLS information, as well as, to restrict access to authorized persons and only for authorized purposes. The FPLS Security Plan will address these safeguards in more detail.

2.1.1 SOCIAL SECURITY ACT, SECTION 453 (42 U.S.C. 653)

The Social Security Act limits access to the NDNH data to the following:

1. State agencies that administer the Child Support program, the Temporary Assistance for Needy Families (TANF) program, the UI program and the Foster Care and Child Welfare programs,
2. the Secretary of the Treasury for purposes of administering the tax laws,
3. the Commissioner of the Social Security Administration for purposes of verifying Social Security numbers and other purposes,
4. researchers pursuing projects likely to contribute to achieving the purposes of the Child Support and TANF programs but without personal identifiers,
5. authorized persons as defined by Section 453(c) and Section 463(d) of the Social Security Act,
6. courts with authority to issue child support orders,
7. the Department of Education for collection of debts, and
8. the Department of Housing and Urban Development (HUD) for determination of eligibility for selected housing programs.

Section 453(m) of the Social Security Act states that the Secretary shall establish and implement safeguards designed to ensure the accuracy and completeness of information in the FPLS and to restrict access to confidential information to authorized persons and for authorized purposes.

2.1.2 THE PRIVACY ACT OF 1974 (P.L. 93-579)

The Privacy Act provides standards for, and restrictions on, records maintained by Federal agencies on individuals.

Section 552a(d) - Access to Records. - Each agency that maintains a system of records shall

- (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;
- (2) permit the individual to request amendment of a record pertaining to him and -
 - (A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and
 - (B) promptly, either -
 - (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or
 - (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;
- (3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;
- (4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and
- (5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

2.1.3 THE COMPUTER SECURITY ACT OF 1987 (P.L. 100-235)

Computer Security Act of 1987 mandates the improvement of privacy for unclassified, sensitive information in Federal computer systems. It requires Federal agencies to prepare, and periodically update, security plans for their computers that process sensitive information. It also requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer practices of all Federal and contractor employees who are involved with the management, use, and operation of each Federal computer system

within or under the supervision of that agency.

2.1.4 OMB BULLETINS AND CIRCULARS

OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

The purpose of this Bulletin is to provide guidance to Federal agencies about computer security planning activities required by the Computer Security Act of 1987. Based on the criteria in the Bulletin, the FPLS is defined as a major application under development.

OMB Circular No. A-130, Security of Federal Automated Information Resources

Appendix III of this Circular establishes a minimum set of controls to be included in Federal automated information security programs. It also assigns Federal agency responsibilities for the security of automated information and links agency automated information security programs and agency management control systems. It also incorporates requirements of the Computer Security Act of 1987 and responsibilities assigned in applicable national security directives.

2.1.5 FIPS PUBLICATIONS

FIPS Pub 73, Guidelines for Security of Computer Applications

This document focuses on controls for use with computer applications and provides guidance to address and prevent inadequacies in the design and operation of computer applications.

FIPS Pub 102, Guidelines for Computer Security Certification and Accreditation

This publication describes how to establish and implement a computer security certification and accreditation program.

2.1.6 DHHS AIS SECURITY PROGRAM HANDBOOK

The DHHS AIS (Automated Information Systems) Security Program Handbook establishes departmental policies, procedures and responsibilities for the implementation and administration of security. It provides references to other security requirements.

2.2 NDNH FPLS Federal and State Level Security

The NDNH System contains sensitive information (W-4, UI and QW), which requires protection from unauthorized disclosure. Due to the sensitivity of the information, the confidentiality protection requirement level is considered to be high. FPLS information is categorized as Level 3 high sensitivity designation as specified in the Department of Health and Human Services (HHS) Automated Information Systems Security Program (AISSP) Handbook. Level 3 data must be protected from unauthorized disclosure, fraud, waste and abuse. The misuse, unauthorized access to, or modification of FPLS information could result in exceptionally grave damage to the program or the privacy to which individuals are entitled

under the Privacy Act. To ensure the privacy of NDNH data and to prevent unauthorized access to this data, there are safeguards in place at the Federal level. In addition to the Federal level security, each state agency must have safeguards to ensure security of data, as described by the above-referenced sources.

2.2.1 NDNH FPLS FEDERAL LEVEL SECURITY

Section 453(l) – Restrictions on Disclosure and Use

Information in the FPLS, and information resulting from comparisons using such information, shall not be used or disclosed except as expressly provided in Section 453 (1) and subject to Section 6103 of the Internal Revenue Code of 1986.

Section 453(m) – Information Integrity and Security

The Secretary shall establish and implement safeguards with respect to the entities established under this section designed to –

- (1) ensure the accuracy and completeness of information in the FPLS; and restrict access to confidential information in the FPLS to authorized persons, and
- (2) restrict use of such information to authorized purposes.

Security for the FPLS at the Federal level includes management controls (such as conducting background investigations on personnel), development/implementation controls (such as design review and testing), operational controls (such as emergency backup, disaster recovery, business continuity and contingency planning), security awareness and training, and technical controls (such as user identification and authentication). The development of these various controls is evolutionary over the life of the system.

The FPLS central processing and data storage are physically located at the Social Security Administration's (SSA) National Computer Center (NCC) in Baltimore, Maryland. Physical and perimeter security safeguards exist to protect personnel, hardware, software, data and other components of the NCC. All agency and contractor personnel are subject to the security awareness and training provisions of the Computer Security Act. Security software will be implemented to further protect the information in the FPLS.

All SSA mainframes at the NCC operate under the TOP SECRET Control System. TOP SECRET provides security to protect computer data from destruction, modification, disclosure and misuse. It controls access of the computer resources and automatically denies and logs unauthorized attempts to access resources. TOP SECRET has the ability to log authorized use of sensitive resources for subsequent review. The SSA/OCSE administrator controls access privileges under TOP SECRET.

Data transmissions from the states to the NCC are via data transmission software, known as CONNECT:Direct, along dedicated lines within SSA's closed network. The Network Control Center, within the NCC, employs sophisticated network monitoring software that assists in identifying unauthorized access. In addition, SSA has installed the Secure Plus encryption

option on all of its platforms, including those that house the FPLS system. States and Federal agencies should install Secure Plus and transmit encrypted data to OCSE.

In order to comply with the privacy safeguards required by the authorities listed above, agreements on privacy, security and the use of FPLS data have been developed between OCSE and the Department of the Treasury, the Social Security Administration, and other entities as appropriate. Their use of the data is restricted as provided by legislation.

Within OCSE, access to the data is limited to those in the FPLS branch, and the Associate Commissioner of the Office of Automation and Program Operations (OAPO). A locking door controls access to the room in which the FPLS is located, with limited key access. A list of approved staff is maintained by the FPLS Security Team and is reviewed on a regular basis by management. Visitors to the room must sign in and be escorted at all times by a staff member with approved access.

2.2.2 STATE LEVEL SECURITY

State SWA systems are responsible to comply with privacy and security safeguards established by the Department of Labor (DoL) and their own respective state laws. SWA Systems have long been in effect and each SWA should ensure compliance with their own requirements. Please refer to the DoL for clarification on specific requirements.

In addition, Section 454A of the Act requires the state agency administering the IV-D program to have in place safeguards on the integrity, accuracy and completeness of, access to, and use of data in the statewide automated system which shall include the following:

1. written policies concerning access to data by state agency personnel, and sharing of data with no other persons;
2. system controls (such as password or blocking of fields) to ensure strict adherence to those policies;
3. routine monitoring of access to and use of the automated system, through methods such as audit trails and feedback mechanisms, to guard against and promptly identify unauthorized access or use;
4. procedures to ensure that all personnel, including state and local agency staff and contractors, who may have access to or be required to use confidential program data are informed of applicable requirements and penalties, including those in Section 6103 of the Internal Revenue Code of 1986, and are adequately trained in security procedures.
5. administrative penalties, up to and including dismissal from employment for unauthorized access to, or disclosure or use of, confidential data.

It is also a State plan requirement in Section 454(26) of the Act that states have in effect safeguards applicable to all confidential information handled by the state agency. These should be designed to protect the privacy rights of the parties and should include:

1. safeguards against unauthorized use or disclosure of information relating to proceedings to establish paternity or to establish, modify or enforce support orders;

2. prohibitions against the release of information on the whereabouts of one party to another party against whom a protective order has been entered;
3. prohibitions against the release of information on the whereabouts of one party to another if the state has reason to believe the release of the information may result in physical or emotional harm to the former party.

The state agency is also required to establish safeguards as the Secretary of Labor may determine necessary to ensure information on wages and claimed is used only for the purposes specified in Section 453(i)(1) of the Act.

3.0 TECHNICAL SUPPORT

The OCSE provides technical and functional support to the submitters of NDNH data. These resources include a telephone number that a user can call to receive assistance for technical or operational problems, and an Internet World Wide Web site address. The following chart shows the resource and contact information.

CHART 3-1: TECHNICAL SUPPORT RESOURCES	
Resource	How to Contact Resource
FPLS Information Line	1-202-401-9267
OCSE FPLS Website	http://www.acf.hhs.gov/programs/cse/newhire

4.0 APPLICATION

As part of the Federal requirements for reporting new hire data, every state must establish an SDNH that receives, transcribes into automated format, conducts automated data matches against IV-D cases in the SCR, and transmits W-4 data to the NDNH. Federal requirements also specify that Federal agencies must format and transmit new hire data directly to the NDNH. In addition to W-4 reporting, the Federal agencies and states must report QW information to the NDNH, and the states must also report UI information to the NDNH.

For W-4, UI, Federal agency QW data and QW data submitted by a state that stores and transmits full employee names, the NDNH System processing first transmits the data to SSA to verify the accuracy of the SSN and its related name against information resident in the SSA database. When the NDNH receives notification that the SSN is verified, the system then adds the data to the NDNH database.

For further information about SSN processing, refer to Section 5.0, “Social Security Number Verification”.

4.1 Strategic Issues

Reporting of NDNH information requires the coordination and cooperation of multiple public and private organizations and businesses at the Federal, state, and local levels. Organizational structures and processing capabilities vary significantly from one Federal agency to another and from one state to another. The Social Security Act allows Federal agencies and states the flexibility to design their new hire programs in a manner most compatible with the strengths and capabilities of each particular Federal agency or state. These variations create challenges in building an effective network that supports the operational aspects of on-going new hire reporting.

4.1.1 OVERSIGHT INITIATIVES

Because responsibility for the reporting of W-4, QW and UI data may reside in different agencies (e.g., SWAs, Child Support Enforcement IV-D agencies, contractor organizations, data processing centers), states may want to consider forming a committee that develops and recommends operational guidelines under which the reporting of data to the NDNH occurs. Some of the strategic issues to consider are:

1. The development and maintenance of interagency agreements that specify responsibilities of the different parties involved in reporting to the NDNH;
2. The establishment of frameworks under which the programs operate;
3. The coordination and direction of:
 - a) employer outreach, compliance, and accuracy for W-4 reporting,
 - b) initiatives for improvement of reporting of data,
 - c) staff training, including customer service, data preparation, data processing, and technical support,
 - d) fraud detection for Unemployment Insurance benefits and Workers’ Compensation,

- e) reviewing system components to ensure goals and objectives are being met, and
- f) information dissemination about progress of the NDNH to interested parties (employers, participating agencies, etc.) and to inform the general public of the program's impact on child support enforcement and fraud detection.

4.1.2 STATE SYSTEM INTEGRATION STRATEGIES

Each state's integration strategy must take into account the state's existing structure, organizational arrangement and level of automation. Business processes of data gathering, information processing and communication with the NDNH depend on the locale of the SDNH, automated system capabilities and communication links between the system(s) that process the QW, UI and W-4 data. A system may be a composite of records containing all the information (W-4, QW and UI) for transmission to the NDNH, or, it may be a data transfer configuration that collects data from different points of origin, maps them to the appropriate format and transmits the files to the NDNH. Regardless of the system configuration, there are basic common factors. The list below contains some of the factors states should address in program operations. While these are not all-inclusive, they offer material for consideration by state planners.

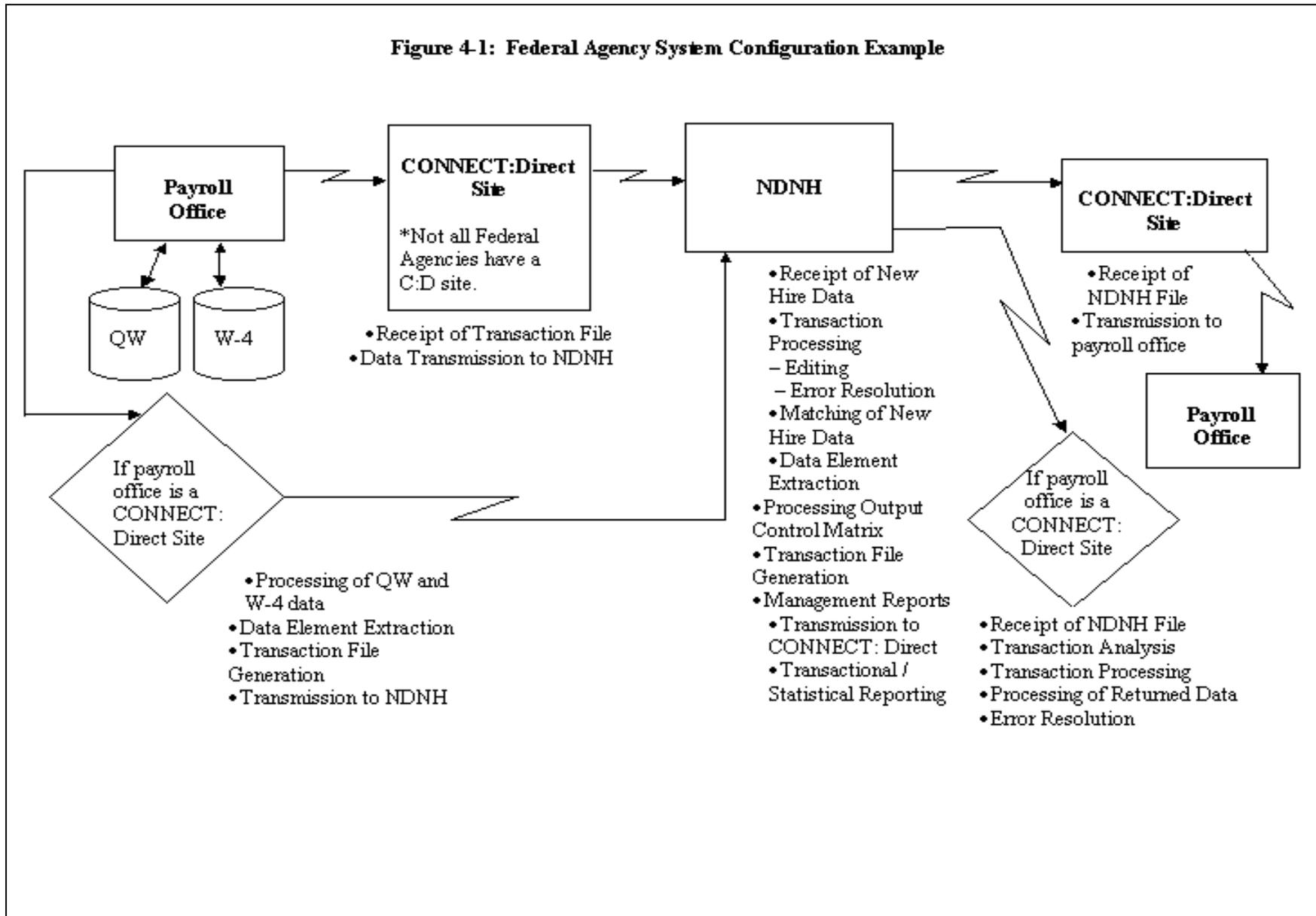
1. Establishment of procedures for data entry functions:
 - a) W-4 data may be transmitted by employers to the SDNH via many different means, such as by paper, telephone, magnetic or electronic processes. Transcription of the data to a single automated format will be necessary for transmission to the NDNH;
 - b) Methods for error resolution at point of data entry or through automated editing at system entry;
 - c) Scheduling of processing steps to ensure that Federal timeframes are met, particularly during peak processing periods, such as transmission of QW and UI data.
2. Modification of existing systems or development of new systems:
 - a) Procedural and business requirements for the interface with the NDNH that reflect the needs of all agencies/entities participating in the state's program;
 - b) Procedural and business requirements that support the automated reporting of data to ensure all Federal programmatic requirements are met;
 - c) Modification of existing systems or development of new systems to meet prescribed requirements; and
 - d) Development of communication links that will support file transfers between hardware components (e.g. data centers) when W-4, QW and UI reside in different systems or agencies that transport the data to the CONNECT:Direct site.
3. Establishment of policies and procedures for periodic system validation to ensure continuing optimal operation:
 - a) Measuring and analyzing user satisfaction and the perceived validity of the data;
 - b) Measuring and assessing system availability and timely delivery of scheduled outputs and activities;
 - c) Control of data access to ensure that adequate safeguards are in place for data security and confidentiality to protect against misuse, while allowing access to authorized persons/entities; and
 - d) Measuring and assessing employer compliance.

4.2 System Configuration

4.2.1 FEDERAL AGENCY SYSTEM CONFIGURATION EXAMPLE

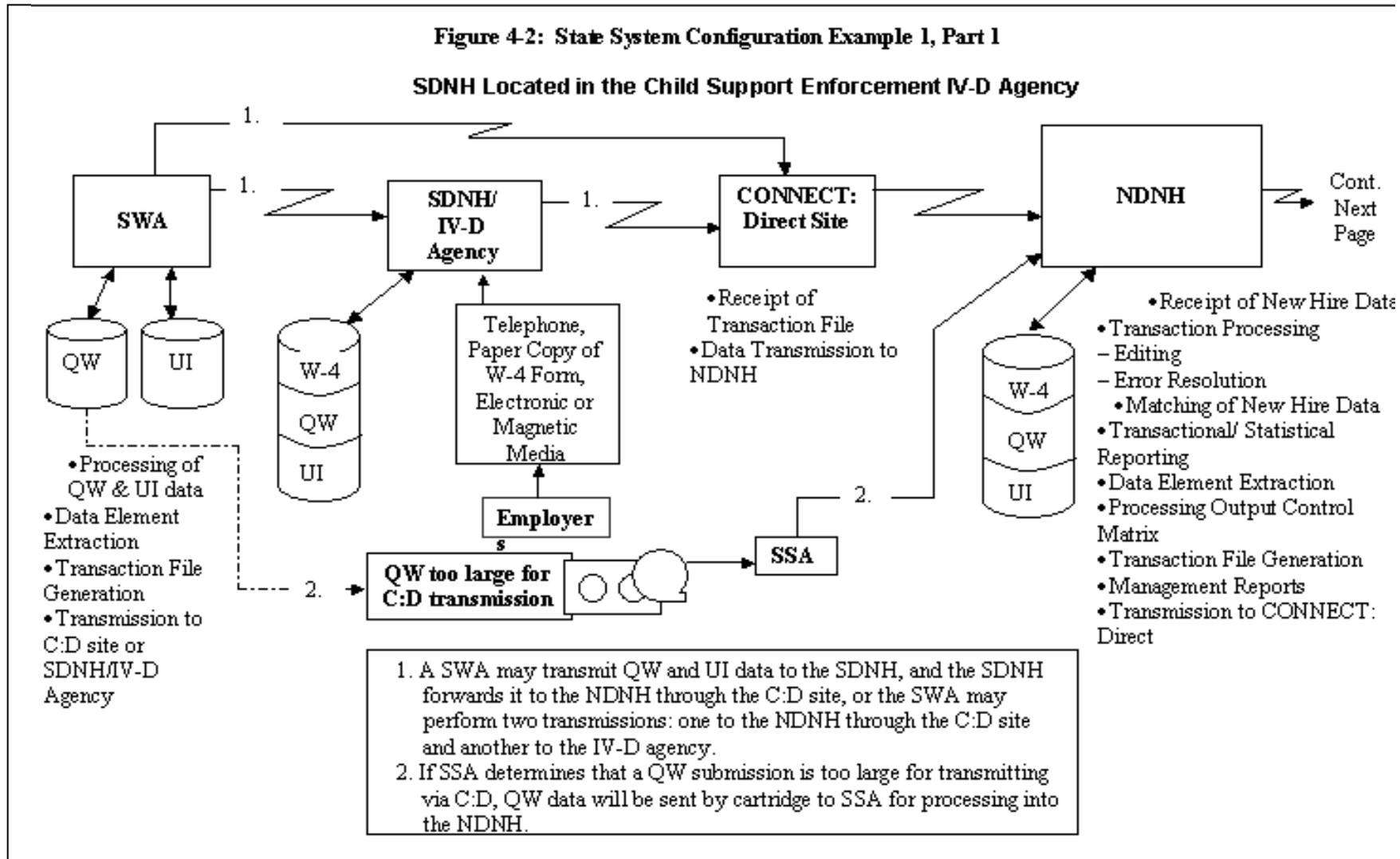
Figure 4-1 provides an example of a typical Federal agency configuration.

Figure 4-1: Federal Agency System Configuration Example



4.2.2 STATE SYSTEM CONFIGURATION EXAMPLES

The following diagrams provide examples of typical state configurations.



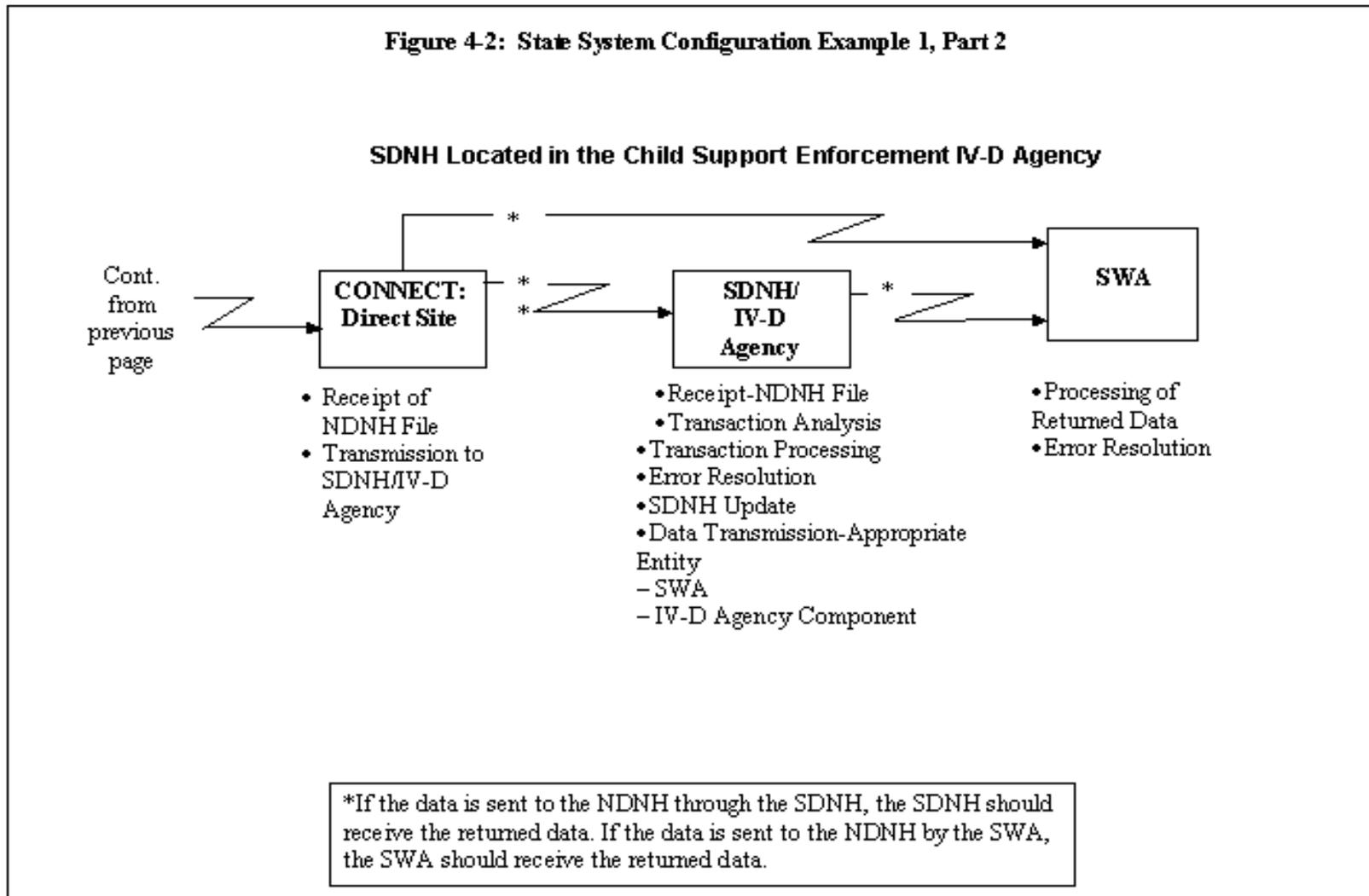


Figure 4-3: State System Configuration Example 2, Part 1

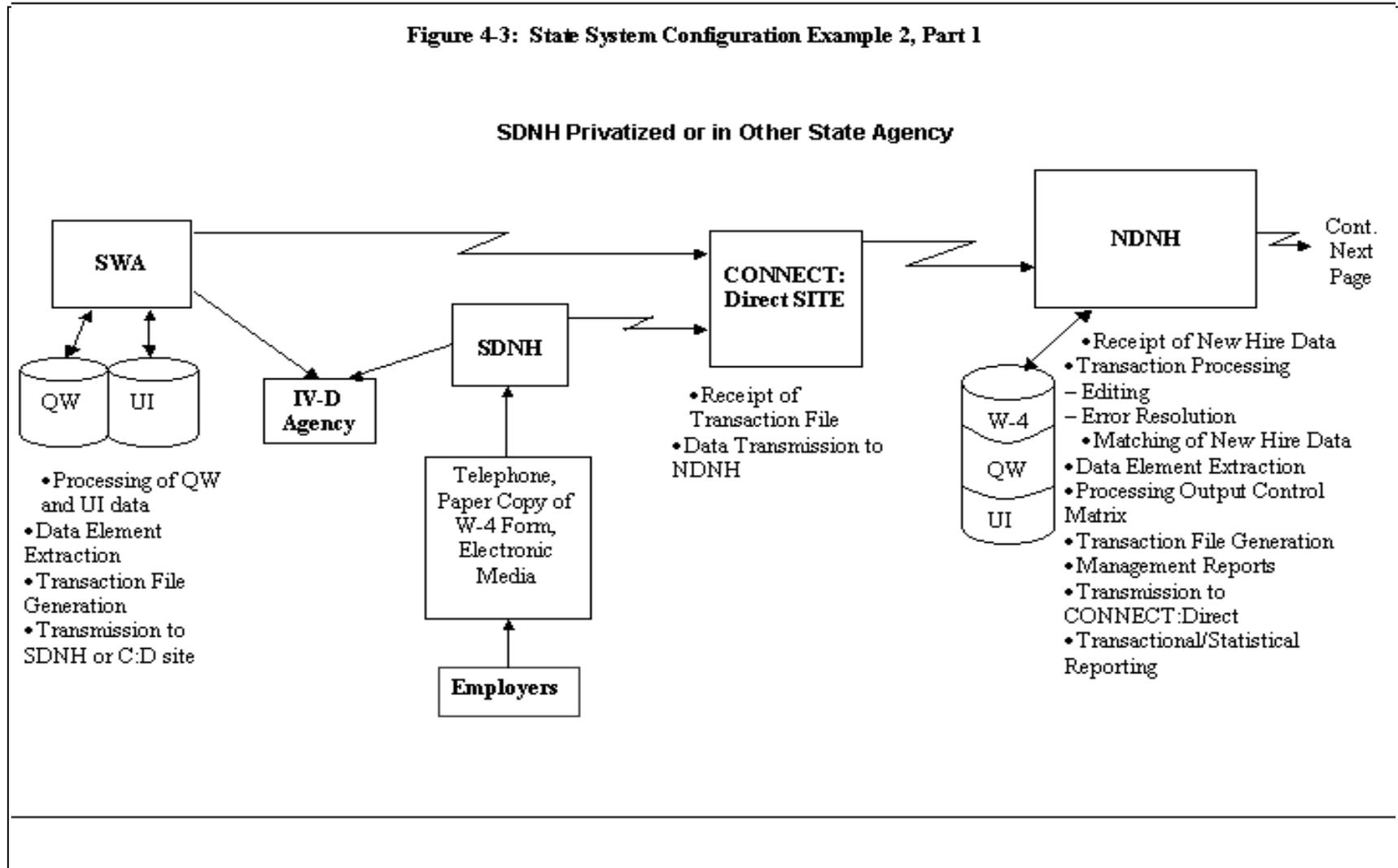
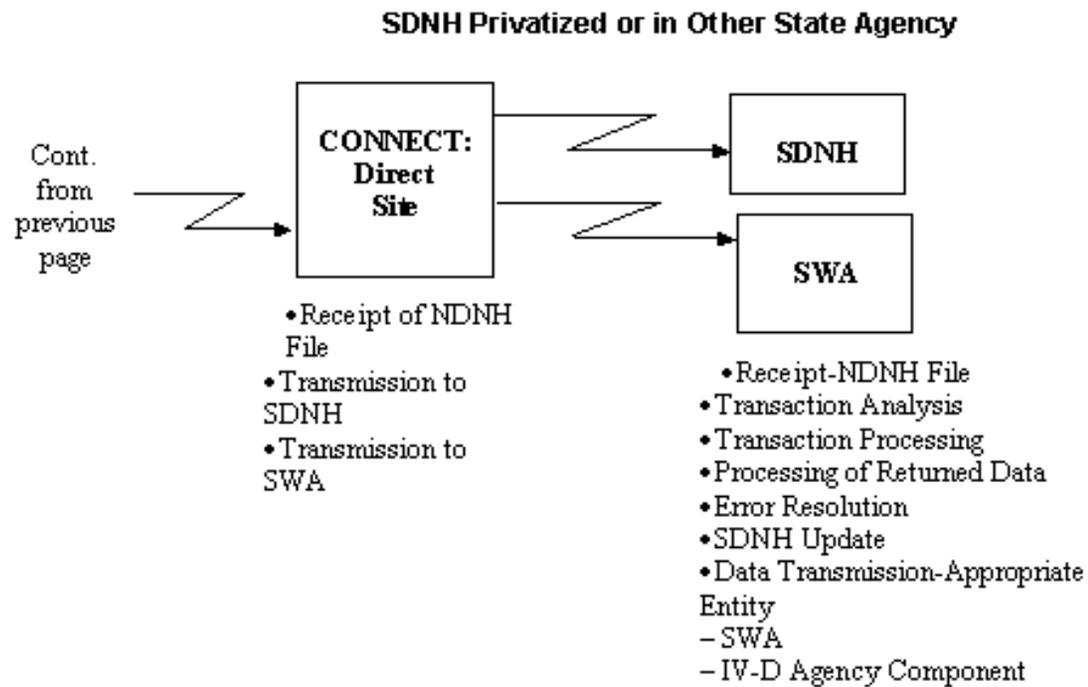
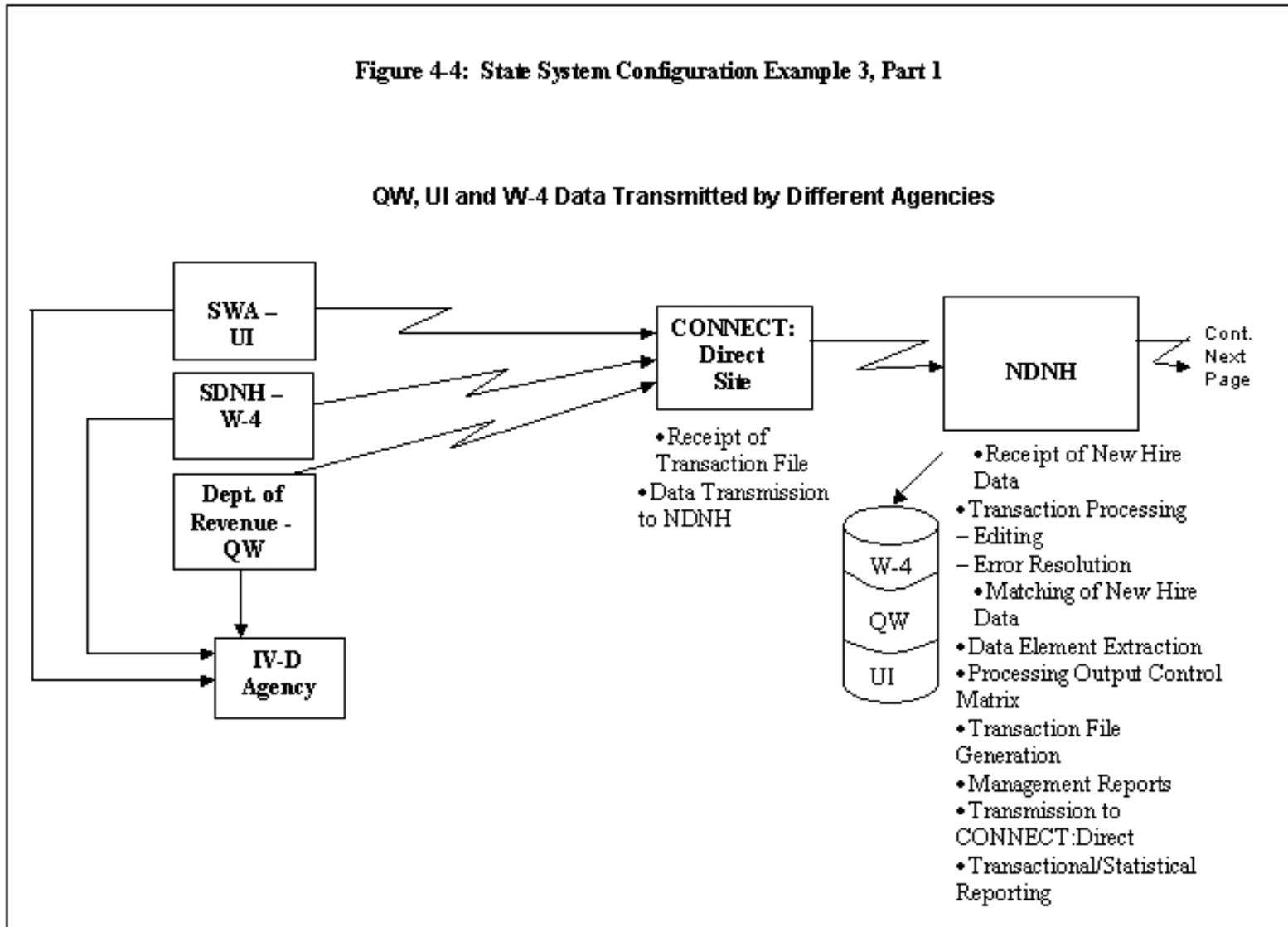
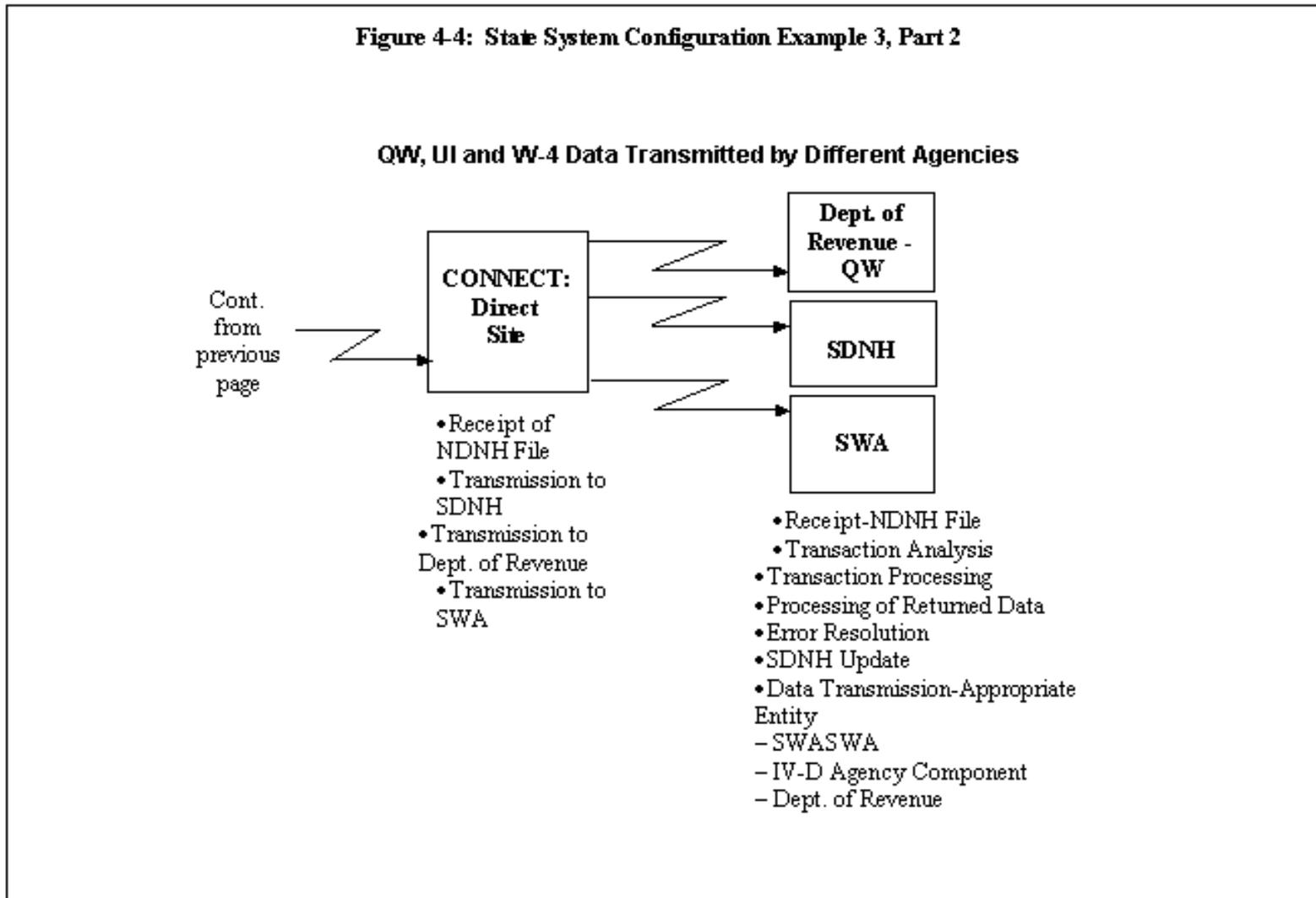


Figure 4-3: State System Configuration Example 2, Part 2







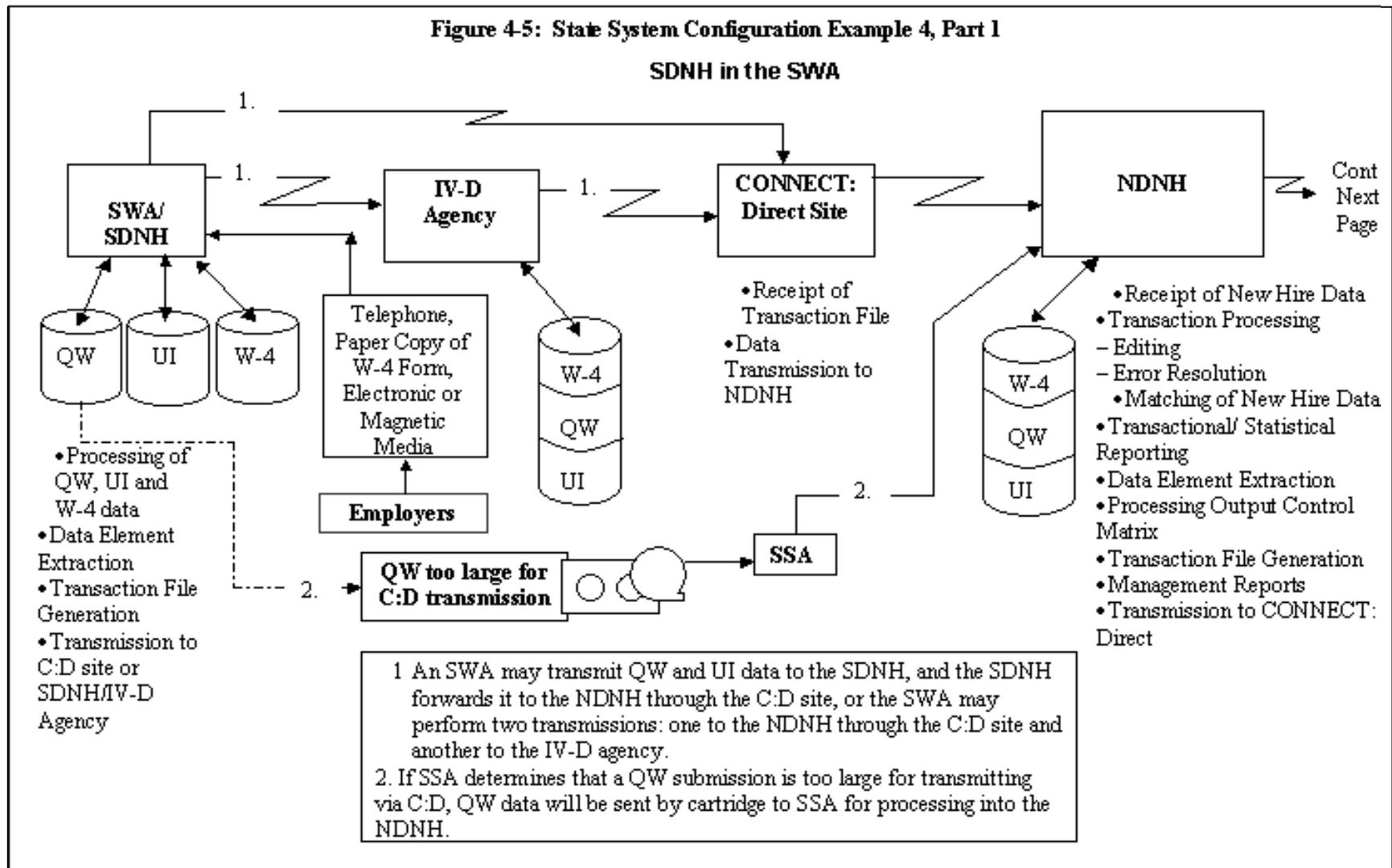
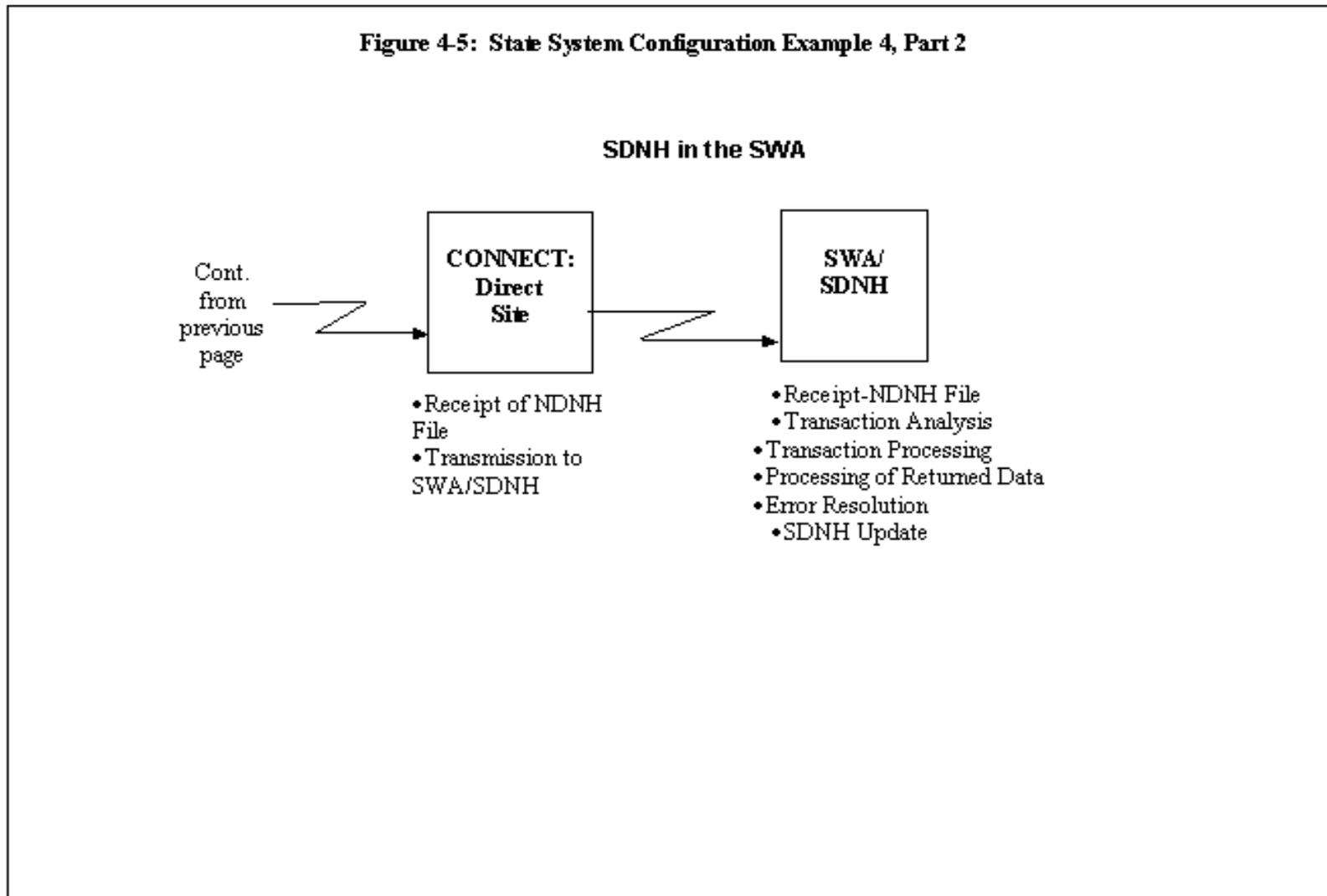


Figure 4-5: State System Configuration Example 4, Part 2



5.0 SOCIAL SECURITY NUMBER VERIFICATION

Upon receipt of W-4, QW and UI from States or W-4 and QW from Federal agencies, the NDNH System transmits the data to SSA, which attempts to verify the SSN and its related name against information resident in the SSA database. There are several outcomes of this verification process and the submitting agency receives notification of the results, as requested in the NDNH Output Control Matrix Registration. Refer to the sections on W-4, QW or UI Output for more information regarding the matrix and the data that is available for return to submitting agencies.

The submitting agency receives a summary of the SSN results and may also choose to receive the errors, warnings and corrections on individual records. The SSN process checks the submitted SSN and name for the following:

1. Is the SSN a possible number issued by SSA? (W-4, QW and UI)
2. Do the SSN and name submitted on the record match the SSN and name on SSA's records? (W-4, QW and UI)
3. Does the SSN have a number transposition and need correction? (W-4 only)
4. Does the SSN have incorrect digits and need correction? (W-4 only)

If SSA verifies an SSN on a W-4, QW or UI record, or corrects an SSN on a W-4 record, the NDNH System then posts the record to the NDNH Database. If SSA processing corrects the SSN, the record posts to the NDNH Database with the corrected SSN.

Note: SSNs are shown in format ###-XX-####.

5.1 Rejected SSNs

There are several conditions that cause SSNs to be rejected. SSN errors may be due to general edits, or errors found during the SSN verification process. Listed below are conditions that generate rejected SSNs:

1. The SSN is non-numeric.
2. The SSN is missing.
3. The SSN is invalid or out of range.
4. The SSN on the record has a name and SSN that do not match, or the SSN is not found.

The submitter of the W-4, QW or UI data receives notification of these errors in the transmission acknowledgement. Federal agencies must correct the errors and resubmit the records. State agencies are encouraged to correct the errors and resubmit the records, but are not required to do so. Refer to the W-4, QW or UI "Data Validation and Verification", Sections 11.0, 19.0, and 27.0, for the error and warning codes associated with the above SSN errors.

SSNs containing invalid characters and spaces are rejected, as well as those SSNs that have

not been assigned through SSA. W-4, QW and UI records must contain SSNs that are properly formatted in order to successfully pass the SSN verification process.

If an SSN is invalid, the system rejects the record and notifies the submitting agency that the SSN is invalid.

Example: The SSN submitted with the record is 888-XX-8888.

- The system identifies 888-XX-8888 as a number that has not been issued by SSA,
- The system rejects the record, and
- Generates a notification to the submitting agency that 888-XX-8888 is not an SSN issued by SSA.

5.2 Non-Matching SSN/Name Combinations

Non-matching SSN/Name combinations are defined as those that do not correspond to SSA's assigned SSN and name combinations. W-4, QW and UI records must contain SSNs and names that match SSA's records, in order to successfully pass the SSN verification and identification process.

If an SSN and name combination does not match SSA's SSN and name combination, the system rejects the record and notifies the submitting agency that the SSN and name do not match.

Example: The SSN and name submitted with a record are 333-XX-9911 and Dave Jones.

- The system verifies that the name assigned to 333-XX-9911 is not Dave Jones,
- The system rejects the record, and
- Generates a notification to the submitting agency that the SSN and name for this record do not match.

5.3 Corrected SSNs (W-4 Only)

The W-4 validating routines have the capability to identify SSNs that have transposed digits or that have minor numerical errors, such as having one incorrect digit in the SSN. The system selects a corrected SSN only if it can identify one, and only one, corrected SSN/Name combination for the person. The system stores the corrected SSN on the NDNH database with an indicator showing that the SSN is corrected, and notifies the submitting agency of the correction. **Do not resubmit SSNs that are corrected as a result of the NDNH SSN processing.**

Example: The SSN and name submitted with a W-4 record are 285-XX-9999 and Linda Kay.

- The system verifies that the correct SSN for Linda Kay is 258-XX-9999.
- The system stores Linda Kay with the correct SSN, 258-XX-9999, with an indicator that the SSN has been corrected.

- The system generates a notification to the submitting agency that Linda Kay's correct SSN is ~~258~~-XX-9999.

Example: The SSN and name submitted with a W-4 record are 383-XX-7633 and Don Campbell.

- The system verifies that the correct SSN for Don Campbell is 383-XX-6633.
- The system stores Don Campbell with the correct SSN, 383-XX-6633, with an indicator that the SSN has been corrected.
- The system generates a notification to the submitting agency that Don Campbell's correct SSN is 383-XX-6633.

5.4 Non-Verifiable SSNs

Some State's QW records include only a partial set of letters or no letters in the employee's name(s). When these States send their records to the NDNH, the system checks the SSN to determine if it is within the range of SSNs issued to date by SSA. Records with SSNs outside the issued range are rejected. If the SSN is within the range, the system attempts verification. If the SSN/Name combination does not verify, the system accepts the record and stores it on the QW Non-verifiable File.

Example: A State that only stores a partial set of letters for employee names submitted a QW record with an SSN and name of 274-XX-0154 and "Ge" and "McD" in the first and last name fields.

- The system verifies that 274-XX-0154 is within the range of SSNs issued to date by SSA.
- The system is unable to verify the SSN/Name combination, so it accepts the record and stores the SSN 274-XX-0154 and the partial employee name "Ge McD" on the QW Non-Verifiable File.

5.5 Transposing First and Last Names

If a QW or W-4 record contains an SSN/Name combination that passes SSA's "High Group check" but does not verify with SSA, the NDNH will reverse the order of the First Name and Last Name and resubmit that name with the SSN to see if this new SSN/Name combination verifies. If the SSN does verify with the transposed names, the NDNH will accept and store the record with the names transposed and return Warning Code **0004** to the submitter. If the transposed name and SSN do not verify, then the originally-submitted name and the SSN are returned with Error Code **0001**.

6.0 CONNECT:Direct TRANSMISSION

Federal and state agencies transmit W-4, QW and UI data using SSA's network and the CONNECT:Direct (C:D) protocol. CONNECT:Direct is a data transfer software product that allows data centers within and across networks to send and receive large amounts of data via mainframe-to-mainframe data exchange. The W-4, QW and UI records transmitted to the NDNH via CONNECT:Direct must be in the appropriate record format. **Each dataset name must be unique and may contain a valid Transmission Date in YYMMDD format.** The date in the dataset name should be the current date. Dataset names that contain an invalid date or an incorrectly formatted date cause unnecessary processing. If the state or Federal agency abbreviation in the incoming dataset name does not correspond to that field's value in the Transmitter Header Record, the file is rejected and no return notification is sent to the submitter. However, the Technical Support (TS) team informs the submitter by phone. Refer to the relevant transmission sections (W-4, QW or UI) for data requirements, data format rules, record layouts and field descriptions.

6.1 CONNECT:Direct Strategic Issues

Currently, a network exists and is operated through SSA that connects each state and some Federal agencies to SSA. Each state has a copy of the CONNECT:Direct product for submitting data via the SSA network. Each state has one data center within the network. In addition, many Federal agencies have been issued a copy of the CONNECT:Direct product for submitting data to the SSA, and there are several Federal data centers within the network.

The Administration for Children and Families (ACF) has a formal agreement with SSA, which allows Federal agencies and states to send and receive data through SSA's existing network.

The basic element of CONNECT:Direct is a file transfer process. Transfers are initiated by submitting predefined processes consisting of a single 'COPY' statement or combinations of multiple statements separated by conditional logic. Processes can trigger transfers at a requested time under predetermined criteria. Six different activities may be specified in a process:

1. Move files among systems;
2. Submit jobs;
3. Execute programs;
4. Submit other processes;
5. Build and resolve symbolic values; and
6. Alter the sequence of process execution through conditional logic.

CONNECT:Direct has a checkpoint/restart feature. It eliminates the need to retransmit an entire file in the event of a transmission failure. If a transfer error occurs, the CONNECT:Direct software automatically restarts transmission at the most recent checkpoint. The CONNECT:Direct also automatically generates on-line statistics for security, auditing

and accounting purposes. This allows Federal agencies and states to determine usage of network resources and to determine how to improve network efficiency.

The following steps must be taken to begin using the CONNECT:Direct network to transmit NDNH data:

1. Identify the data center that is connected to the SSA CONNECT:Direct network.
2. Identify the person responsible for creating the CONNECT:Direct process to transmit data.
3. Determine the data center's CONNECT:Direct type (Hub, Spoke, Type-4 Spoke).
4. Distribute the appropriate CONNECT:Direct form and sample Job Control Language (JCL) to the CONNECT:Direct contact. Complete this form and submit it to the Federal technical liaison. Federal programmers use the information on this form to create the CONNECT:Direct processes. The sample JCL provides instructions to the programmer and supplies examples of how to create the necessary CONNECT:Direct process to submit NDNH data.
5. Create the CONNECT:Direct processes (JCL) necessary to submit data to the NDNH.
6. Enter the necessary CONNECT:Direct Point of Entry (POE) security parameters.
7. Contact the technical liaison to schedule a test to determine the success of submitting and receiving data from the NDNH. A list of the technical liaisons is available through the Technical Support Customer Service Hotline or from the OCSE's World Wide Web Internet Home Page. The telephone number for the Hotline and the Web address are in the CONNECT:Direct Technical Support table of this Guide.

6.1.1 CONNECT:Direct SECURE+

OCSE has provided all NDNH submitters that use CONNECT:Direct with a copy of CONNECT:Direct Secure+, which is a comprehensive, cryptographic security solution, which is approved by the National Institute of Standards and Technology (NIST). Secure+ encrypts and decrypts data transmitted to and from the NDNH via CONNECT:Direct.

CONNECT:Direct users must install and activate Secure+ at their site. Chart 6-1, "CONNECT:Direct Technical Support", which follows, provides the phone number and e-mail address to which questions regarding Secure+ installation should be directed.

The following pages contain Figure 6-1, "SSA CONNECT:Direct Registration Form", and the instructions for completing the form.

SSA CONNECT:Direct REGISTRATION FORM	
REQUEST DATE: ____/____/____ TRANSFER TYPE: SPOKE: ____ HUB: ____ TYPE 4: ____	
STATE: _____ C:D NODE NAME: _____	
STATE C:D CONTACT: _____ PHONE NUMBER: () _____	
HUB STATES ONLY:	
NETWORKING CONTACT: _____ PHONE: () _____	
VTAM NETID: _____ VTAM C:D APPLID: _____ VTAM HOST CDRM: _____	
SSA TRANSFER TO SSA	
<p style="text-align: center;">DSN FROM STATE</p> <p>DISP=____ UNIT=____ VOL=SER=____</p>	<p style="text-align: center;">DSN TO SSA</p> <p>OLBG.BTO.UIN.FPLS.Sss.Rdate Where sss = state code; date = YYMMDD</p> <p>or</p> <p>OLBG.BTO.xcxIN.FPLS.sss.Time.Rdate Where xcx = W-4 or QW sss = Federal agency code; or 'S' + state code time = MMSSHH date = YYMMDD</p>
SSA TRANSFER TO STATE	
<p style="text-align: center;">DSN FROM SSA</p>	<p style="text-align: center;">DSN TO STATE</p> <p>DISP=____ UNIT=____ VOL=SER=____</p> <p>DESTINATION UNIT TYPE: TAPE: _____ DASD: _____</p>
<p>OLBG.BTI.sss.xcxOUT.FPLS.Rdate Where sss = Federal agency code; or 'S' + state code xcx = W-4, QW, UI date = YYMMDD</p>	
STATE C:D READ/WRITE USERID/PWD: _____	
STATE C:D CREATE USERID/PWD: _____	
SPECIAL INSTRUCTIONS: _____	

Instructions on how to fill out the CONNECT:Direct registration form.

REQUEST DATE: The date the form is being filed out.

TRANSFER TYPE: Select the version of C:D that you have.

STATE: The name of your state or Federal agency.

C:D NODE NAME: Input the unique Node-Name of your system.

STATE C:D CONTACT: The name of the contact person for C:D in your location.

PHONE NUMBER: C:D contact person's phone number.

NETWORKING CONTACT: Networking contact name (If different than C:D contact).

PHONE: His/her phone number

Virtual Telecommunication Access Method Information:

VTAM NETID:

VTAM C:D APPLID:

VTAM HOST CDRM:

STATE TRANSFER TO SSA:

DSN FROM STATE: The file name on the State's or on the Federal agency's computer where the data resides.

DISP: The status of the file and what is to be done with the file after notification of successful transmission: SHR is the default.

(FROM) DISP = ([OLD | SHR]
, [KEEP | DELETE]
, [KEEP | DELETE])

UNIT: The unit address or device type where the file resides on the State or Federal agency system.

UNIT = ([unit-address | device-type | group-name | unit-count | P])

VOL=SER: The specific physical location of the file to be transferred to SSA.

VOL=SER=(serial-no, [serial-no, ...])

SSA TRANSFER TO STATE:

DSN TO STATE: The file name on the State or Federal agency system to which the SSA will write the data.

DISP: Status of the File on the receiver node.

(TO) DISP = ([NEW | OLD | RPL | SHR]
, [KEEP | CATALOG]
, [KEEP | CATALOG | DELETE])

UNIT: The unit address or the device type on the State's system or on the Federal agency's system where the file resides.

UNIT = ([unit-address | device-type | group-name | unit-count | P])

VOL=SER: The specific physical location of the file to be transferred to SSA.

VOL=SER=(serial-no, [serial-no, ...])

DESTINATION UNIT TYPE (TAPE / DASD): The destination type of media.

STATE C:D READ /WRITE USER ID/PWD: The ID and PWD to be used by the State or Federal agency when submitting C:D processes.

STATE C:D CREATE USER ID/PWD: ID and PWD to be used by SSA for testing.

SPECIAL INSTRUCTIONS: Any additional comments that you consider necessary.

6.2 Sample JCL for CONNECT:Direct

Federal agencies and states may use the following sample JCL for building the job for transmitting NDNH data files to the SSA Data Center. Substitute your own values for the CONNECT:Direct Dataset names. As this is just a sample, other information may require modification to conform to your data center environment.

6.2.1 SAMPLE JCL

```
//JOBSEND JOB
(OCSE,XYX), 'NDNHXMIT', CLASS=E, MSGCLASS=T, NOTIFY=XYX
//*
//DMBATCH EXEC PGM=DMBATCH, REGION=1M, PARM=( YYSLYNN)
//STEPLIB DD DISP=SHR, DSN=SYS3.NDM.STAND.LOADLIB
//DMNETMPA DD DISP=SHR, DSN=SYS3.NDM.STAND.NETMAP
//DMPUBLIB DD DISP=SHR, DSN=SYS3.NDM.STAND.PROCESS.LIB
//DMMSGFIL DD DISP=SHR, DSN=SYS3.NDM.STAND.MSG
//DMPRINT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//NDMCMD5 DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD *

SIGNON SUBMIT PROC=SENDNH NOTIFY=XYX
&RUNDATE=970820
SIGNOFF
/*
//
```

Place the following process, SENDNH, into the PDS library referenced by the above DMPUBLIB DD statement. Note: Substitute your agency or state name where the Snn appears. Substitute your C:D Node Name for PNODE= .

```
SENDNH PROCESS PNODE=NDM.SGA.Snn SNODE=NDM.SSA.NCC
*
STEP1 SUBMIT DSN=NDMNCC.Snn.PROCESS.LIB(W4IN) -
SUBNODE=SNODE -
&RDATE=&RUNDATE
```

6.3 CONNECT:Direct Technical Support

Federal and state agencies can receive technical support regarding the C:D process and protocols. These resources include a telephone number that a user can call to receive assistance for technical questions or problems and an Internet World Wide Web site address. The following chart shows the resource and contact information.

CHART 6-1: CONNECT:Direct TECHNICAL SUPPORT	
Resource	How to Contact Resource
FPLS Information Line	1-202-401-9267
CONNECT:Direct User Guide	http://www.acf.hhs.gov/programs/cse/newhire/library/transmission/transmission.htm
Data Transmission Team	http://www.acf.hhs.gov/programs/cse/newhire/contacts/dttcontacts.htm
CONNECT:Direct Secure+ Information	Jim Fox (410-965-5634) jfox@acf.hhs.gov

6.4 CONNECT:Direct Summary, Conclusion and Recommendation

C:D is the most expedient and secure method of transmitting NDNH data. Once each Federal agency and state establishes their CONNECT:Direct protocols, data transmission becomes fast and reliable. CONNECT:Direct ensures that the NDNH System receives W-4, QW and UI data in the most timely manner, enabling the Child Support Enforcement IV-D Agencies to use the data quickly and efficiently in child support enforcement efforts.

7.0 DATA RETENTION

The Social Security Act imposes restrictions on access to, and retention of, NDNH data. The Act does not allow HHS to have access to W-4, QW and UI data where 12 months has elapsed since the date the information was provided, and where there has not been a match resulting from the use of the information in any information comparison activity. This statute also requires that all NDNH data to be deleted from the database 24 months after the date of entry into the NDNH. The law does allow the Secretary to retain such samples of data entered into the NDNH as the Secretary finds necessary to assist in carrying out research purposes as specified in section 453(j)(5) of the Act.