DRAFT

CDC

CENTERS FOR DISEASE CONTROL
AND PREVENTION

PRELIMINARY TECHNICAL PLAN

for the

STATE IMMUNIZATION INFORMATION SYSTEM (SIIS)

JUNE 1994

Prepared by:

NISE WEST Code 213
Department of the Navy
Telecommunications and Engineering Division

STATE IMMUNIZATION INFORMATION SYSTEM (SIIS)

TECHNICAL PLAN

JUNE 1994

Approved by: _____

Robert P. Cruz, Department Director
Terrestrial Communications
NISE West Code 210

Approved by: _____

Donald L. Eddins, Director
Division of Data Management
National Immunization Program

TABLE OF CONTENTS

Section	Title	Page
1.0	GENERAL REQUIREMENTS	1-1
1.1	Introduction	1-1
1.2	Background	1-2
1.3	State Immunization Information System (SIIS) Plan Development	1-3
1.4	References	1-3
1.5	Compatibility With Existing Systems	1-4
	1.5.1 Proposed State Immunization Information System (SIIS)	1-4
	1.5.2 Provider Data Entry into the SIIS	1-4
	1.5.3 Intrastate and Interstate Data Transmission	1-4
	1.5.4 SIIS Database Size	1-8
	1.5.5 Internet History	1-13
1.6	Continuity of Operations	1-14
1.7	Security Requirements	1-14
	1.7.1 Guidelines for Security Issues	1-14
	1.7.2 Encryption In Network Access Control	1-15
1.8	Schedule	1-15
2.0	SCOPE	2-1
2.1	Facilities	2-1
2.2	Network Electronics	2-2
2.3	Responsibilities	2-2
	2.3.1 NISE West San Diego	2-2
	2.3.2 National Immunization Program Function	2-6
	2.3.3 State Project Director/Program Manager	2-7
3.0	ELECTRONIC SYSTEM DESIGN AND INSTALLATION	3-1
3.1	System Design	3-1
3.2	System Description	3-2
	3.2.1 Equipment Descriptions	3-2
	3.2.2 Hardware Interface Requirements	3-5
3.3	Hardware Warranties	3-5

TABLE OF CONTENTS (cont)

Section	Title	Page
3.4	SIIS Drawings	3-5
4.0	SOFTWARE	4-1
4.1	ORACLE7 Features	4-1
4.2	Software Features	4-3
	4.2.1 Database Structure	4-5
4.3	Internetworking Software	4-7
4.4	Network Management Software	4-7
4.5	Terminal Emulation Software	4-7
4.6	Network Test Software	4-7
4.7	Software Licensing Agreements	4-7
5.0	ELECTRONIC EQUIPMENT	5-1
5.1	Operational Electronic Equipment	5-1
5.2	Electronic Test Equipment	5-1
6.0	NETWORK/SYSTEM CHECKOUT AND ACCEPTANCE	6-1
6.1	General Requirements	6-1
6.2	Standards	6-1
6.3	Individual Equipment Tests	6-2
6.4	Overall System Tests	6-3
7.0	PHYSICAL PLANT	7-1
7.1	General Information	7-1
7.2	Power Requirements	7-1
7.3	Telephone/Internet Service	7-1
7.4	Environmental Control	7-2
7.5	Fire Protection	7-2
7.6	Grounding	7-2

TABLE OF CONTENTS (cont)

APPENDIX

Appendix	Title
A	GLOSSARY OF INTERNETWORKING TERMS
B	ACRONYMS AND ABBREVIATIONS
C	NATIONAL IMMUNIZATION PROGRAM (NIP) AND NISE WEST POINTS OF CONTACT
D	NISE WEST/NATIONAL IMMUNIZATION PROGRAM (NIP) CONSULTANTS/PROJECT OFFICER REGIONAL ASSIGNMENTS

TABLE OF CONTENTS (contd)

LIST OF FIGURES

Figure	Title	Page
1-A	SIIS BLOCK DIAGRAM	1-5
1-B	INTERNET/NSFNET DIAGRAM	1-6
1-C	NETWORKS CONNECTED TO THE U.S. INTERNET	1-7
1-D	SITE IMPLEMENTATION SCHEDULE	1-16
2-A	EXAMPLE OF A STATE HUB NETWORK CONFIGURATION	2-3
2-B	EXAMPLE OF A STATE HUB EQUIPMENT RACK	2-4
3-A	HARDWARE INTERFACE CONNECTOR DIAGRAM	3-6

TABLE OF CONTENTS (contd)

LIST OF TABLES

Table	Title	Page
1-1	TYPES OF VACCINE PREVENTABLE DISEASES	1-8
1-2	SAMPLE CHILDHOOD IMMUNIZATION SCHEDULE	1-9
1-3	SIIS DATABASE SIZE	1-11
4-1	CORE DATA SET INDIVIDUAL IDENTIFICATION	4-5
4-2	CORE DATA SET IMMUNIZATION TRANSACTION	4-6
4-3	CORE DATA SET VACCINATION CODE CROSS REFERENCE	4-6
5-1	ELECTRONIC EQUIPMENT PROCUREMENT	5-2
5-2	ELECTRONIC TEST EQUIPMENT REQUIREMENTS	5-3
6-1	EQUIPMENT/CERTIFICATION CROSS REFERENCE	6-1
7-1	EQUIPMENT CHARACTERISTICS TABULATION	7-3

SECTION ONE

1.0 GENERAL REQUIREMENTS

1.1 Introduction

A primary goal of the National Immunization Program (NIP) is to ensure that at least 90 percent of all children born on or after 1 October 1996, receive age appropriate vaccinations.

To reach this goal, NIP is sponsoring the establishment of the State Immunization Information System (SIIS) to assist all states and U.S. territories in performing vaccination follow-up, recording events, and monitoring vaccine distribution and use.

The SIIS has two components: the Record Exchange Interface (REI) and the Record Management System (RMS). Together they form a system to collect and maintain immunization information and exchange that information between states. The SIIS communicates between clinics and providers across the nation using the Internet networking system.

The SIIS software will be a Windows New Technology (NT)-based operating system software with "point and click" techniques. The SIIS will create, store and retrieve immunization records, and track vaccine inventories.

SIIS Record Management System (RMS) data records can be requested from one state's database and sent to another state's database.

The State Immunization Information System (SIIS) Technical Plan provides an economical and technically feasible approach for integrating data systems within states to collect and summarize immunization data.

The SIIS Program requirements are detailed in Paragraph 1.4.

1.2 Background

The purpose for the SIIS technical plan is to provide guidance for implementing a SIIS in each state and U.S. territory by September 30, 1999:

- A system that ensures the adequate vaccination of at least 90 percent of all children born on or after October 1, 1996.
- A system that ensures the follow-up of children who miss scheduled vaccinations.
- A secure and confidential system that enables appropriate health care providers within states to access a child's vaccination record.
- A system that monitors adverse events to immunizing agents.
- A system that monitors vaccine distribution and usage.

Based upon the information received in the SIIS Needs Assessments, most states and U.S. territories do not currently have automated systems capable of meeting the above requirements. Several states have automated information systems in the public sector and another small number of states have plans to automate their record keeping and follow-up systems.

The concept of an integrated, automated network should be maintained because of its ultimate effectiveness across multiple health and social program lines. In this type of system development, coordination and collaboration will be crucial.

1.3 State Immunization Information Systems (SIIS) Plan Development

Each state was tasked to conduct a Needs Assessment and to report the results to the National Immunization Program (NIP) by January 17, 1994. One purpose of the Needs Assessment is to provide baseline information for developing a plan to implement an automated State Immunization Information System (SIIS). The Needs Assessment will serve as the basis for the plan to develop a comprehensive statewide system. This SIIS Technical Plan outlines a design concept which can be implemented to meet NIP objectives in every state within the specified period of time.

1.4 References

a) Senate of the United States Bill S.732 (Comprehensive Child Immunization Act of 1993) dated 1 April 1993; "To Provide for the immunization of all children in the United States against Vaccine-Preventible diseases and for other purposes."

b) Centers for Disease Control (CDC) and Prevention, National Immunization Program, Data Management Division, Systems Development Branch, Version 2.5, by Larry Blumen. Subject: Proposal for the State-wide Immunization Information System (SIIS).

c) Inter-Agency Agreement Between NCCOSC ISE West Coast Division and Centers for Disease Control and Prevention, National Immunization Program dated November 1993.

d) National Science Foundation (NSF) Network News, September 1993, Number 13.

1.5 Compatibility With Existing Systems

1.5.1 Proposed State Immunization Information System (SIIS)

The proposed State Immunization Information System (SIIS) is diagrammed on Figure 1-A. See Appendix A for a list of internetworking terms and Appendix B for a list of acronyms.

1.5.2 Provider Data Entry into the SIIS

Each immunization provider (private doctor, local hospitals, community health centers, or rural clinics) will report to the state central database via a data entry device. The various providers will be equipped with a variety of input devices. These input devices may be: facsimile (FAX) machines, personal computers (PCs) with modems, and large main frames with modems. Each state hub will have to accommodate these different types of input devices.

1.5.3 Intrastate and Interstate Data Transmission

Intrastate and Interstate data transmission will be accomplished by existing telephone service and/or by the Internet. Principle Internet nodes are shown on Figure 1-B. Figure 1-C shows the numbers of networks connected to the Internet backbone and the names of public and private service providers. The SIIS data transfer will use Transmission Control Protocol (TCP)/Internet Protocol(IP) network protocol on Internet.

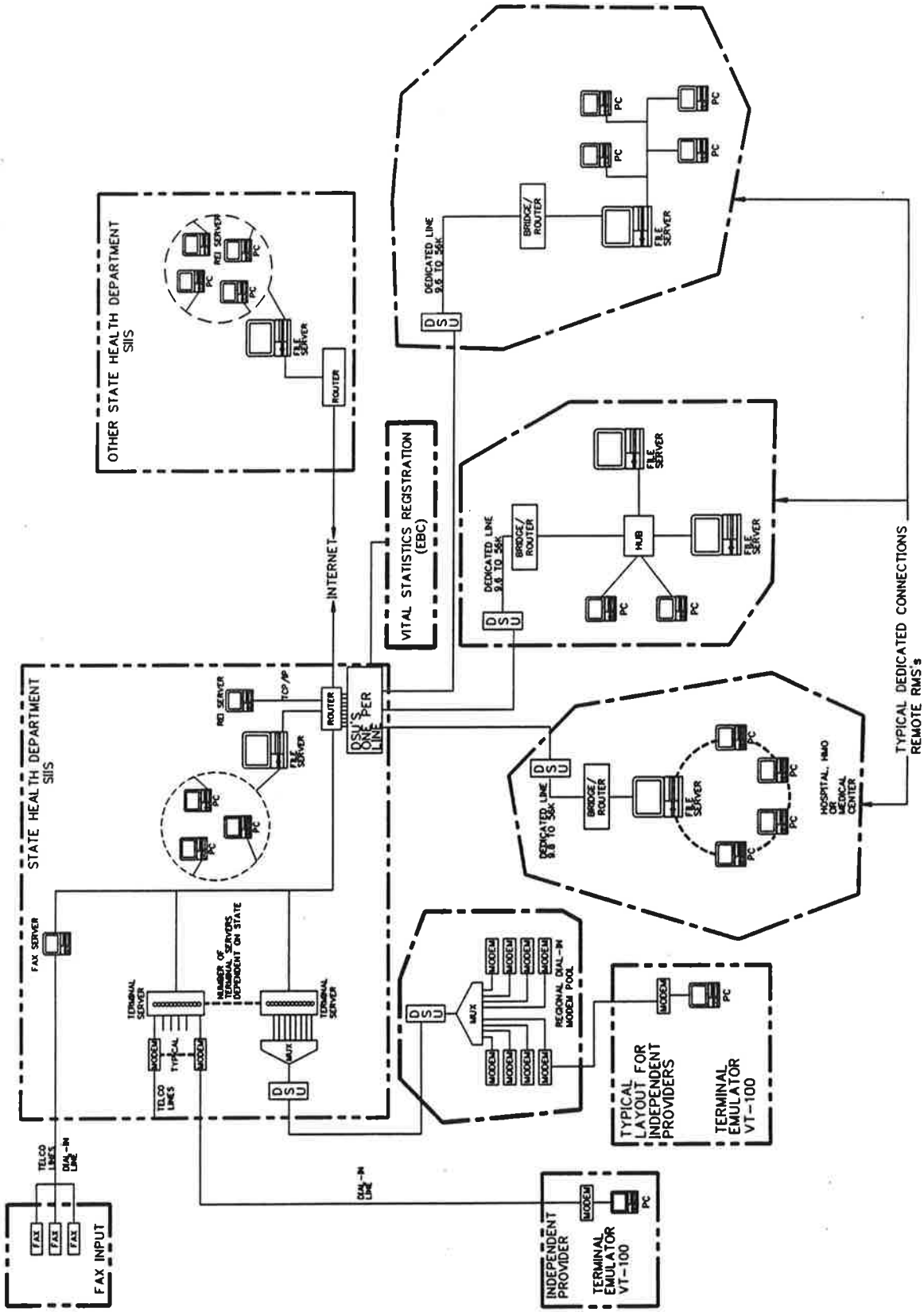


Figure 1-A SIIS BLOCK DIAGRAM

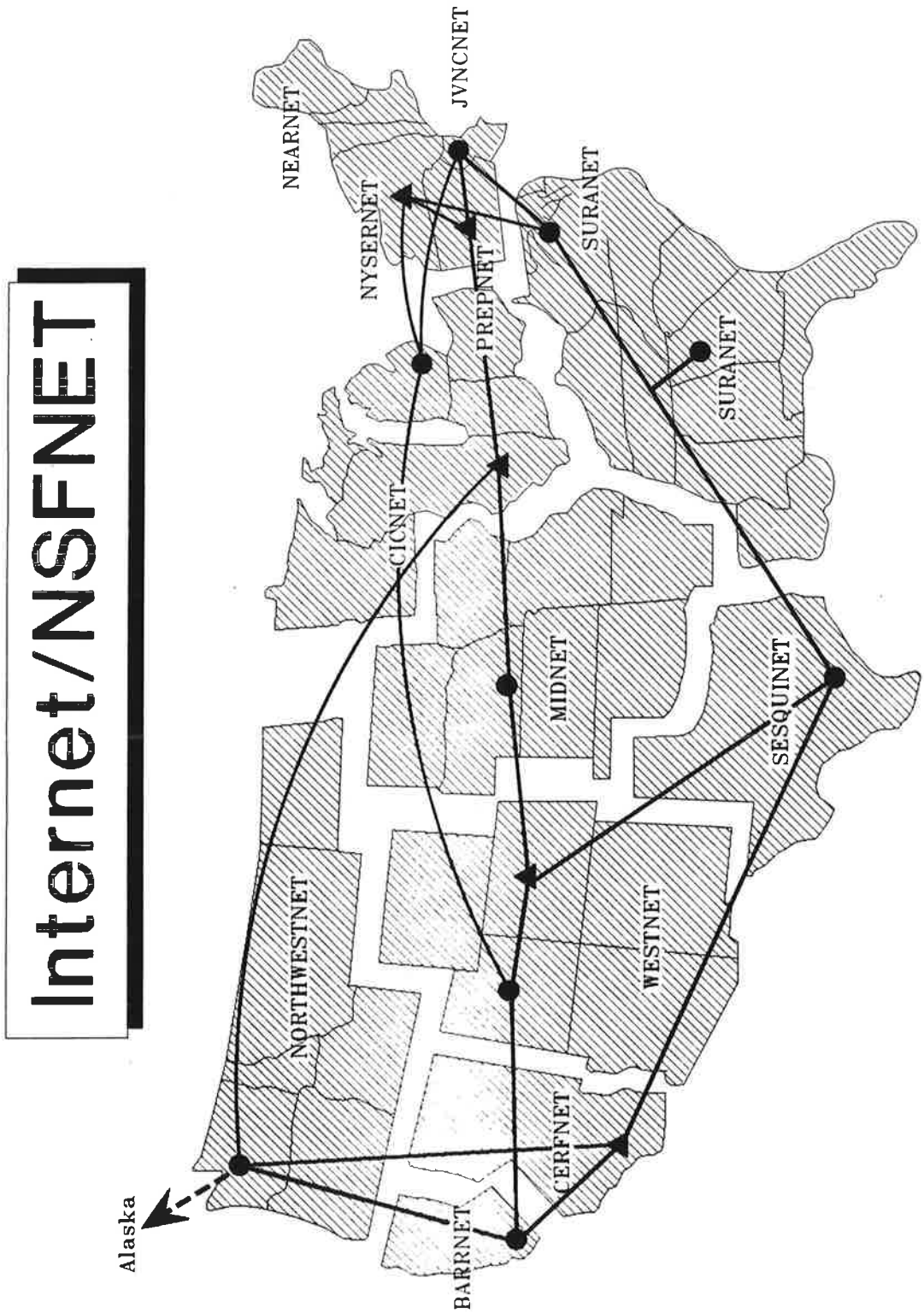


Figure 1-B INTERNET/NSFNET DIAGRAM

STATE	SERVICE PROVIDERS
Alabama	SURAnet
Alaska	NorthWestNet
Arizona	WestNet
Arkansas	MIDnet
California	BARRNet, CERFnet, CSUnet, SDSCnet, Los Nettos
Colorado	CO Supernet, WestNet
Connecticut	NEARnet
Delaware	SURAnet
District of Columbia	SURAnet
Florida	SURAnet
Georgia	SURAnet
Hawaii	PACCOM
Idaho	MIDnet, NorthWestNet, WestNet

STATE	SERVICE PROVIDERS
Illinois	CICNet, netIllinois
Indiana	CICNet, Inet
Iowa	CICNet, MIDnet
Kansas	MIDnet
Kentucky	SURAnet
Louisiana	SURAnet
Maine	NEARnet
Maryland	SURAnet
Massachusetts	NEARnet
Michigan	CICNet, Merit/MichNet
Minnesota	CICNet, MRNet
Mississippi	SURAnet
Missouri	MIDnet
Montana	NorthWestNet

STATE	SERVICE PROVIDERS
Nebraska	MIDnet
Nevada	NevadaNet
New Hampshire	NEARnet
New Jersey	JvNCnet
New Mexico	WestNet
New York	NysernNet
North Carolina	CONCERT, SURAnet
North Dakota	NorthWestNet
Ohio	CICNet, PSCnet, OARnet
Oklahoma	MIDnet
Oregon	NorthWestNet
Pennsylvania	PSCNET, PREPnet
Puerto Rico	SURAnet
Rhode Island	NEARnet

STATE	SERVICE PROVIDERS
South Carolina	SURAnet
South Dakota	MIDnet
Tennessee	SURAnet
Texas	SESQUINET, THEnet
Utah	WestNet
Vermont	NEARnet
Virginia	SURAnet, VERnet
Washington	NorthWestNet
West Virginia	PSCnet, SURAnet, WVNET
Wisconsin	CICnet, WiscNet
Wyoming	NorthWestNet, WestNet

National and International Service Providers
Alternet, ANS, JvNCnet, PSInet, SprintLink

Figure 1-C NETWORKS CONNECTED TO THE U.S. INTERNET

1.5.4 SIIS Database Size

It is recommended that each child receive approximately 20 vaccinations by his/her 5th birthday. Table 1-1 and Table 1-2 lists the types of vaccine preventable diseases and a sample childhood vaccination and immunization schedule.

TABLE 1-1

TYPES OF VACCINE PREVENTABLE DISEASES

VACCINATION	DISEASE PREVENTED
DTP	Diphtheria is a serious infection of the nose and throat and can be fatal. Tetanus (lockjaw) results when a wound is infected by bacteria which releases toxins causing uncontrollable muscle spasms. It can be fatal. Pertussis (whooping cough) is marked by severe, often violent, coughing spells. It can be fatal or cause brain damage.
OPV	Polio is a disease that can cause paralysis and death.
Hepatitis B	Hepatitis is an infection of the liver that causes the skin to turn yellow. It can cause cirrhosis of the liver and liver cancer.
MMR	Measles is a serious childhood disease that can cause pneumonia and encephalitis (inflammation of the brain). This can lead to convulsions, mental retardation or death. Mumps causes fever, headache and swelling of the glands in the cheeks. It can also cause encephalitis, deafness and in older boys can cause sterility. Rubella (German measles) causes a fever, rash and swollen glands in the neck. Occasionally, it can cause encephalitis. If rubella occurs in the first three months of pregnancy, it can cause birth defects.
Hib	Haemophilus influenza type b causes meningitis (an infection on the covering of the brain), pneumonia and infections in the bloodstream, joints, bones, soft tissues, ears, throat and the covering of the heart. Death or permanent brain damage may result.

TABLE 1-2

SAMPLE CHILDHOOD IMMUNIZATION SCHEDULE

AGE	VACCINATION	DOSE #
At Birth	Hep B	1
2 Months	DTP	1
	OPV	1
	Hib	1
	Hep B	2
4 Months	DTP	2
	OPV	2
	Hib	2
6 Months	DTP	3
	Hib	3
6 - 18 Months	Hep B	3
	Hib	4
15 Months	MMR	1
	Hib	4
15 or 18 Months	DTP	4
	OPV	3
4 - 6 Years	DTP	5
	OPV	4
	MMR	2

The SIIS Database size transferred via the Internet has been determined using the following information provided by the National Immunization Program (NIP):

In Reference 1.4b, the National Immunization Program (NIP) has defined a core data set to be used as a guideline with elements most likely to be needed in creating and maintaining such a system. From the

documentation provided by NIP the core data set for one child (with one immunization record - (approximately 44 bytes) can be estimated at 350 bytes. It has been assumed that each child will be receiving 20 immunizations before the age of five. The size of the database for children under age five can be estimated from this formula:

(Core Child Data + (Immunization Transactions * Size of Transaction) * Yearly Birth Rate =
Size of the SIIS Database in Bytes

Example of a calculation for the state of Connecticut:

(350 + (20 * 44)) * 47300 = 58.2 Mega bytes (Mb) per year

Table 1-3 lists and compiles the potential size of the total SIIS database for one year. By using a 56 kilo bytes (kb) per/second (sec) rated network, it would take 25.6 hours (hrs) to transfer the total annual database. The calculation is shown below:

National Total for One Year
(50 States plus U.S. Territories)

5151.2 Mb * 1 Sec/56 kb * 1 Hr/3600 Sec = 5151200000/201600000
= 25.6 Hrs required for total data transfer

The total data transfer could be accomplished in just over one day. The remaining 364 days would represent system idle time. Operationally the SIIS will only require 56 kilo byte per/second transfer rates to accomplish its transfer of immunization information.

TABLE 1-3

SIIS DATABASE SIZE

REGION	STATE	BIRTH RATE (X1000) (YEAR 1992)	MEGABYTES PER YEAR	INTERNET PROVIDERS	DATA RATE
1	CONNECTICUT	47.3	58.2	NEARNET	9.6 kb - 10 Mb
1	MAINE	15.6	19.2	NEARNET	9.6 kb - 10 Mb
1	MASSACHUSETTS	88.1	108.4	NEARNET	9.6 kb - 10 Mb
1	NEW HAMPSHIRE	15.7	19.3	NEARNET	9.6 kb - 10 Mb
1	RHODE ISLAND	14.8	18.2	NEARNET	9.6 kb - 10 Mb
1	VERMONT	7.6	9.4	NEARNET	9.6 kb - 10 Mb
2	NEW JERSEY	119.9	147.5	JVNC NET	19.2 kb - 1.5 Mb
2	NEW YORK	285.6	351.3	NYSER NET	9.6 kb - 1.5 Mb
2	PUERTO RICO	66	81.2	SURA NET	56 kb - 1.5 Mb
2	VIRGIN ISLANDS	2.5	3.1	SURA NET	56 kb - 1.5 Mb
3	DELAWARE	10.9	13.4	SURA NET	56 kb - 1.5 Mb
3	MARYLAND	76.2	93.7	SURA NET	56 kb - 1.5 Mb
3	PENNSYLVANIA	165.2	203.2	SURA NET	56 kb - 1.5 Mb
3	VIRGINIA	97.6	120.1	SURA NET	56 kb - 1.5 Mb
3	WEST VIRGINIA	22.1	27.2	SURA NET	56 kb - 1.5 Mb
3	WASHINGTON D.C.	10.1	12.4	SURA NET	56 kb - 1.5 Mb
4	ALABAMA	63.0	77.5	SURA NET	56 kb - 1.5 Mb
4	FLORIDA	192.3	236.5	SURA NET	56 kb - 1.5 Mb
4	GEORGIA	111.4	137.0	SURA NET	56 kb - 1.5 Mb
4	KENTUCKY	53.9	66.3	SURA NET	56 kb - 1.5 Mb
4	MISSISSIPPI	43.5	53.5	SURA NET	56 kb - 1.5 Mb
4	NORTH CAROLINA	103.0	126.7	SURA NET	56 kb - 1.5 Mb
4	SOUTH CAROLINA	56.6	69.6	SURA NET	56 kb - 1.5 Mb
4	TENNESSEE	74.0	91.0	SURA NET	56 kb - 1.5 Mb
5	ILLINOIS	192.5	236.8	CIC NET	56 kb - 1.5 Mb
5	INDIANA	83.8	103.1	CIC NET	56 kb - 1.5 Mb
5	MICHIGAN	138.9	170.9	CIC NET	56 kb - 1.5 Mb
5	MINNESOTA	65.5	80.6	CIC NET	56 kb - 1.5 Mb
5	OHIO	169.0	207.9	CIC NET	56 kb - 1.5 Mb
5	WISCONSIN	69.9	86.0	CIC NET	56 kb - 1.5 Mb

TABLE 1-3 (cont)

SIIS DATABASE SIZE

REGION	STATE	BIRTH RATE (X1000) (YEAR 1992)	MEGABYTES PER YEAR	INTERNET PROVIDERS	DATA RATE
6	ARKANSAS	34.9	42.9	MID NET	56 kb - 1.5 Mb
6	LOUISIANA	72.0	88.6	SURA NET	56 kb - 1.5 Mb
6	NEW MEXICO	28.5	35.1	WEST NET	56 kb - 1.5 Mb
6	OKLAHOMA	47.8	58.8	MID NET	56 kb - 1.5 Mb
6	TEXAS	373	458.8	SESQUINET	8.6 kb - 1.5 Mb
7	IOWA	38.1	46.9	CIC NET	56 kb - 1.5 Mb
7	KANSAS	37.5	46.1	MID NET	56 kb - 1.5 Mb
7	MISSOURI	75.4	92.7	MID NET	56 kb - 1.5 Mb
7	NEBRASKA	23.0	28.3	MID NET	56 kb - 1.5 Mb
8	COLORADO	54.6	67.2	WEST NET	56 kb - 1.5 Mb
8	MONTANA	11.5	14.2	NORTHWEST NET	56 kb - 1.5 Mb
8	NORTH DAKOTA	8.9	11.0	NORTHWEST NET	56 kb - 1.5 Mb
8	SOUTH DAKOTA	11.3	13.9	MID NET	56 kb - 1.5 Mb
8	UTAH	37.4	46.0	WEST NET	56 kb - 1.5 Mb
8	WYOMING	6.8	8.4	NORTHWEST NET	56 kb - 1.5 Mb
9	ARIZONA	66.7	82.0	WEST NET	56 kb - 1.5 Mb
9	CALIFORNIA	601.0	739.2	CSU NET	56 kb - 1.5 Mb
9	HAWAII	19.9	24.5	PACCOM	64 kb - 1.5 Mb
9	NEVADA	22.3	27.4	NEVADA NET	56 kb - 1.5 Mb
9	AMERICAN SAMOA	1 *	1	PACCOM	64 kb - 1.5 Mb
9	GUAM	1 *	1	PACCOM	64 kb - 1.5 Mb
9	MARSHALL ISLANDS	1 *	1	PACCOM	64 kb - 1.5 Mb
9	MICRONESIA	1 *	1	PACCOM	64 kb - 1.5 Mb
9	NORTHERN MARIANAS	1 *	1	PACCOM	64 kb - 1.5 Mb
9	PALAU	0.4	0.5	PACCOM	64 kb - 1.5 Mb
10	ALASKA	11.7	14.4	NORTHWEST NET	56 kb - 1.5 Mb
10	IDAHO	17.5	21.5	MID NET	56 kb - 1.5 Mb
10	OREGON	41.6	51.2	NORTHWEST NET	56 kb - 1.5 Mb
10	WASHINGTON	79.3	97.5	NORTHWEST NET	56 kb - 1.5 Mb
TOTAL			5151.2		

1.5.5 Internet History

The Internet is a worldwide system of computer networks. It is comprised of thousands of separately administered networks of many sizes, architecture, topology, and types. Each of these networks may connect as many as several thousand host computers. The total number of individual users of the Internet is in the millions. Internet began in the mid-1960s as an United States Defense Department network called the Advanced Research Projects Agency Network (ARPAnet). The ARPAnet was an experimental network designed to support research on packet switched networks.

Advanced Research Projects Agency Network (ARPAnet) continued to function mainly as a wide area experimental network (WAN) through the mid-1980's. Procedures were set up to regulate the allocation of network addresses and to create voluntary standards for the network. As local area networks (LANS) became more pervasive, many ARPAnet hosts became gateways to local networks. A network protocol to allow the interoperation of these networks was developed and named the Internet Protocol (IP). Over time, other groups created IP-based networks (National Aeronautical Space Administration [NASA], National Science Foundation [NSF], State and Regional networks). These networks all interoperate because of the Internet protocol standards.

The National Science Foundation Network (NSFNET) was developed in the mid-1980's to foster access to the five national super computing centers established by the National Science Foundation (NSF). NSFNET has grown to become a national backbone network, interconnecting numerous mid-level networks into a nationwide data network of truly impressive scale.

The collection of all of these interoperating networks is the Internet.

1.6 Continuity of Operations

It is imperative that the installation and integration of the interconnecting equipment for the SIIS, be conducted on a not-to-interfere basis with normal operations. Any temporary loss to capabilities will be scheduled around operations and coordinated with site personnel.

1.7 Security Requirements

Various levels of Network/Physical Security must be designed into the SIIS. Physical security is the first level of defense by limiting physical access to the network equipment. Network Passwords which must be entered when prompted before logon to a network system must be allocated. Firewalls between two networks that buffer and screen all information between networks must also be designed into the SIIS. Additional or specific network security requirements should be identified during the state site survey.

Additional physical security procedures are identified in Section 7 of this plan.

1.7.1 Guidelines for Security

The essential recommendations from these guidelines are summarized below to provide a quick overview of security issues that will improve the overall security of computer applications.

- Determine security objectives, the degree of sensitivity, and the vulnerabilities of the application and its data.

- For existing applications, a risk analysis usually uncovers some vulnerabilities that need immediate attention.

- Define security specifications for the application. These should be developed as part of the definition of requirements for the application.

- Design the interfaces of the system so that unnecessary vulnerabilities are avoided and so that the risk exposure is minimized.

- Include in the system design enough basic controls so the vulnerabilities that cannot be avoided are controlled and managed.

- Conclude the design stage with a detailed design review by a team of experts who were not part of the design effort.

- Once the system is operational, ensure that planned security procedures are followed in all the manual activities associated with the system.

- Contingency plans should be developed to assure the integrity of the data processed and the continuity of the applications's critical function.

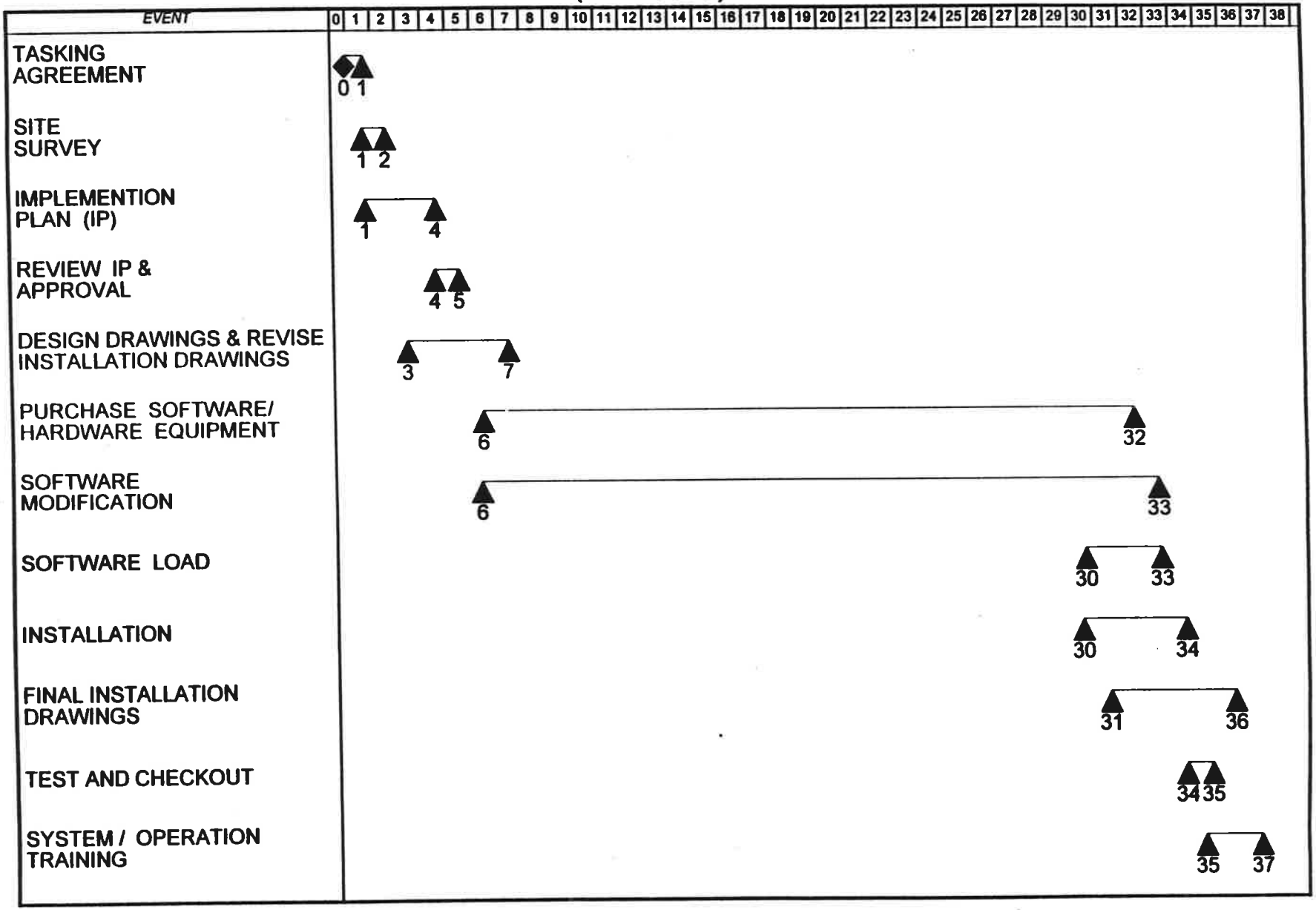
1.7.2 Encryption In Network Access Control

Encryption will be used to preserve the confidentiality of information being transmitted and can aid in safeguarding against various threats such as wiretapping, electronic eavesdropping, misrouting, substitution, modification, and injection of messages. Data files will be safeguarded by encryption techniques. All SIIS information will be encrypted before transmission and decrypted when transmission is received.

1.8 Schedule

A typical implementation schedule is shown in Figure 1-D. The schedule is shown on a weekly basis and the events are all subject to variations depending on individual site requirements and availability of equipment.

SITE IMPLEMENTATION SCHEDULE
(WEEKLY)



NOTE: Subject to variations depending on individual site requirements and availability of equipment.

Figure 1-D SITE IMPLEMENTATION SCHEDULE

SECTION TWO

2.0 SCOPE

This Technical Plan outlines the installation of electronic/network equipment, with software required to establish the State Information Immunization System (SIIS). Installation can consists of File Servers, Routers, Modems, Terminal Servers, FAXs, FAX Servers, MUXs, Data Service Units (DSUs), Personal Computers (PCs) with required cabling. Actual equipment configuration and quantities will be detailed in each Site/State Implementation Plan.

2.1 Facilities

Required facility modifications associated with installation of any new network equipment, will be determined during the state site survey. Any modification of facilities (electrical feeds, outlets, circuit breakers, and wiring) should be coordinated with the state.

Other comments related to facility requirements are contained in Section 7.

2.2 Network Electronics

A typical network configuration is shown in Figure 2-A and Figure 2-B. The actual state site configuration will be defined during the state site survey. The installation portion may include the following:

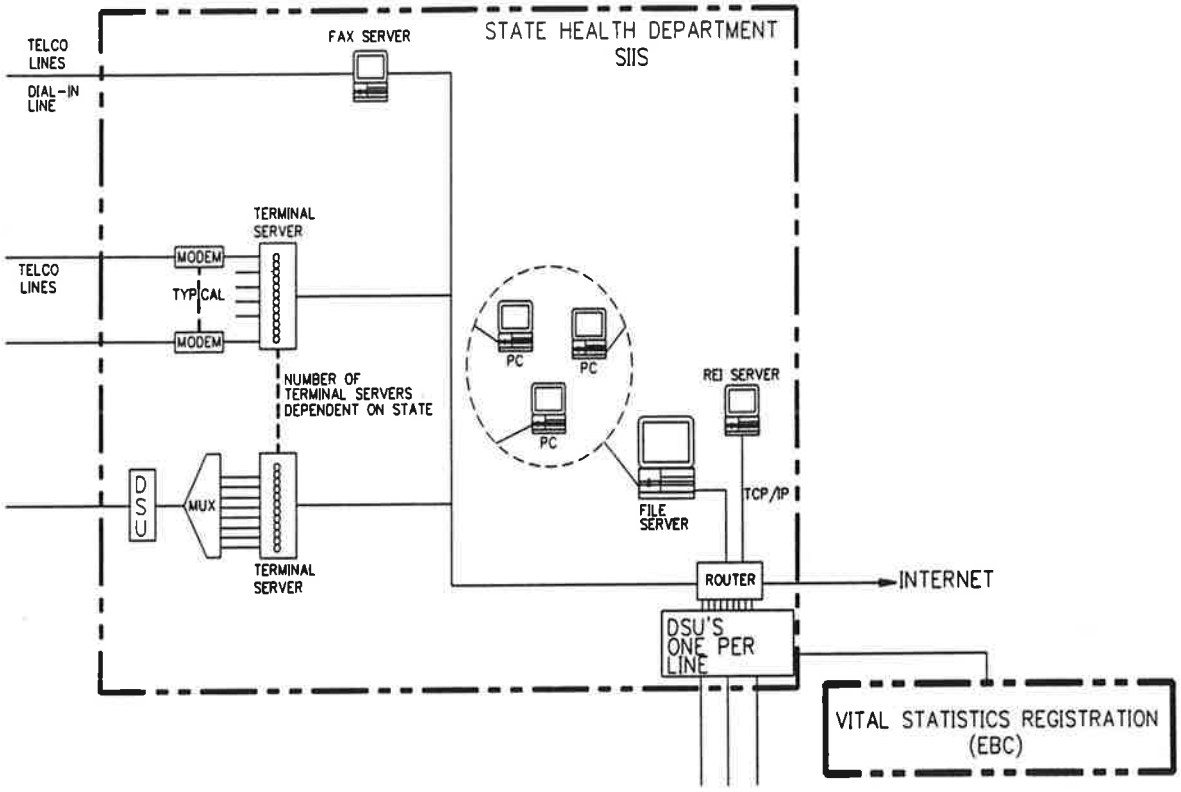
- An equipment cabinet.
- The modems.
- A file server.
- A router.
- A multiplexer.
- Necessary personal computers and Local area Networks (LANs).
- A terminal server.

2.3 Responsibilities

The following paragraphs identifies requirements and responsibilities for each organization involved in this SIIS Technical Plan. See Appendix C for Points of Contact for the SIIS program.

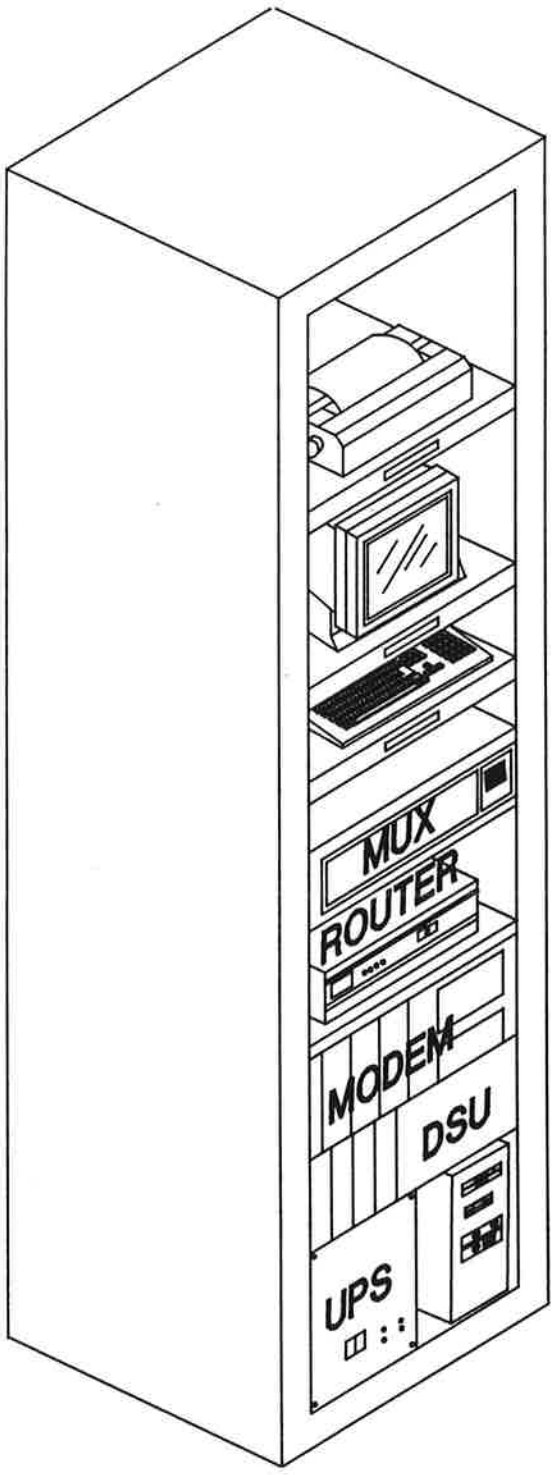
2.3.1 NISE West San Diego

NISE West will provide necessary technical personnel, materials, facilities, and other services needed to support National Immunization Program objectives. Services shall be provided to accomplish specific tasking from the Data Management Division in support of state immunization program initiatives. Such services may include any of the following or related tasks:



Note: Equipment may vary from state hub to state hub.

Figure 2-A EXAMPLE OF A STATE HUB NETWORK CONFIGURATION



Note: Equipment may vary from state hub to state hub.

Figure 2-B EXAMPLE OF A STATE HUB EQUIPMENT RACK

- Conduct surveys of public and private health providers to document existing computing facilities and procedures supporting the documentation and management of immunization events.

- Conduct meetings with state immunization program and data management personnel to discuss and evaluate alternatives for the implementation of State Immunization Information Systems (SIIS) meeting the objectives of the National Immunization Program (NIP) and existing state requirements for immunization data management.

- Evaluate the ability of existing computing facilities at state and local provider levels to support the implementation of the SIIS.

- Provide written assessments of the need for networking hardware, software, personnel and training required to implement the SIIS.

- Prepare cost estimates for procurement of network/system hardware and software, installation and testing services, additional support personnel and training, and any support contract needed to implement the SIIS.

- Prepare plans defining short term and long term objectives for implementation of an SIIS. Plans may include detailed network/system design and functional descriptions, timelines, cost estimates and budget justification for phased implementation, and the impact of delays in implementation of each phase.

- Prepare proposed network/system functional descriptions.

- Prepare proposed network/system design specifications and drawings.

- Procure network/system hardware and software.
- Provide network/system integration, installation and testing.
- Prepare a user's guide.
- Provide manpower planning and curriculae development.
- Provide network/system maintenance and operator training.
- Provide network/system technical drawings.
- Provide configuration control of all data, software and installed configurations.
- Establish a data repository.

All work performed by NISE West San Diego will be conducted in accordance with written tasking orders issued by Data Management Division within the National Immunization Program (NIP) in Atlanta, GA. or as identified with each State Public Health Task agreement.

See Appendix D for a list of NISE West/National Immunization Program (NIP) Consultants/Project Officer Regional Assignments.

2.3.2 National Immunization Program Function

- Provide SIIS Program Funding.
- Provide SIIS Program guidance.
- Define data core set.

2.3.3 State Project Director/Program Manager

- Approve task agreement and supplemental funding.
- Identify specific state requirements.
- Coordinate/provide site facility utilities (phone connections and electrical outlets).
- Provide computer furniture.
- Support NISE West San Diego in the installation and checkout of all equipment.
- Provide network personnel for operator and maintenance training.
- Provide Review and Comments to individual State Implementation Plans.

SECTION THREE

3.0 ELECTRONIC SYSTEM DESIGN AND INSTALLATION

This section contains a summarized design description and summary of installation tasks for a typical SIIS.

3.1 System Design

The system installation design for electronics/network equipment to be utilized in the SIIS shall be in accordance with the applicable sections of the following technical publications:

a. NAVELEX SD D-1640; Drafting Room Manual.
b. MIL-STD-188-124A; Grounding, Bonding and Shielding.
c. Federal Information Processing Standards Publication 94; September 1983; Guideline on Electrical Power for ADP Installations
d. NAVELEX 0101, 110A; Naval Shore Electronic Criteria Handbook, Installation Standards and Practices.
e. ANSI/NFPA 70, National Electrical Code (latest edition).
f. Equipment technical manuals.
g. FCC Rules and Regulations; Part 15, Radio Frequency Devices.
h. FCC Rules and Regulations; Part 18, Industrial Scientific and Medical Equipment.
i. FCC Rules and Regulations; Part 68, Connection of Terminal Equipment to the Telephone Network.
j. UL 478, "Information - Processing and Business Equipment."
k. UL 1459, "Telephone Equipment."

3.2 System Description

3.2.1 Equipment Descriptions

See Figure 1-A for a diagram of the possible Local Area Network (LAN) and Wide Area Network (WAN) topologies for the SIIS.

FILE SERVER

A computer, capable of supporting multiple users, multiple tasking environment, and large capacity memory storage device dedicated to storing SIIS files. This computer is available to the Local Area Network (LAN) and to the rest of the state via phone lines.

MODEM

Contraction of the terms Modulator - Demodulator. A device that allows computer to talk to one another over telephone lines. A device converts digital pulses into frequencies within the audio range of the telephone for data transfer and converts them back into pulses at the receiving side. Independent providers will access the state LAN via modems.

TERMINAL SERVER

A device allowing access to the main file server by multiple users simultaneously. An input/output device designed to send or receive data.

MUX

Multiplexer (MUX) is a device that merges several low-speed transmissions into one high-speed transmission. The regional dial-in modem pool will use a MUX to convert multiple input low-speed transmissions into one high-speed transmission over a single high-speed telephone line.

DATA SERVICE UNIT (DSU)

Data Service Unit (DSU) a communications device that connects an inhouse line to external digital link circuit. The DSU converts data into the required format.

The larger networks will require DSUs to communicate to the central state network.

BRIDGE

A device that connects two networks using the same communications protocol. A device operating at the Open System Interconnection (OSI) data link layer to connect local and wide area networks.

The larger networks will require bridges to communicate over dedicated lines to the central state network.

ROUTER

A device that connects two or more networks. A router selects the appropriate routing of data between networks based on the destination network address.

FAX

Facsimile (FAX) machine is a device that sends and receives pictures and text over a telephone line. FAX machines can be connected to the FAX server at the state central facility and complete document and graphic information can be transferred or inputted.

FAX Server

A computer that accepts FAX input via the telephone line.

HUB

A device that physically connects two or more cables together. The hub is the central point in a star physical topology of a Local Area Network (LAN). Any star topology system will require a hub as the central point of the star.

3.2.2 Hardware Interface Requirements

See Figure 3-A for a diagram of the various Interface cable connections.

3.3 Hardware Warranties

Hardware warranties will be obtained for all equipment.

3.4 SIIS Drawings

A set of drawings for each State Site System will be provided to the site supervisor, by NISE West San Diego, upon completion of the installation.

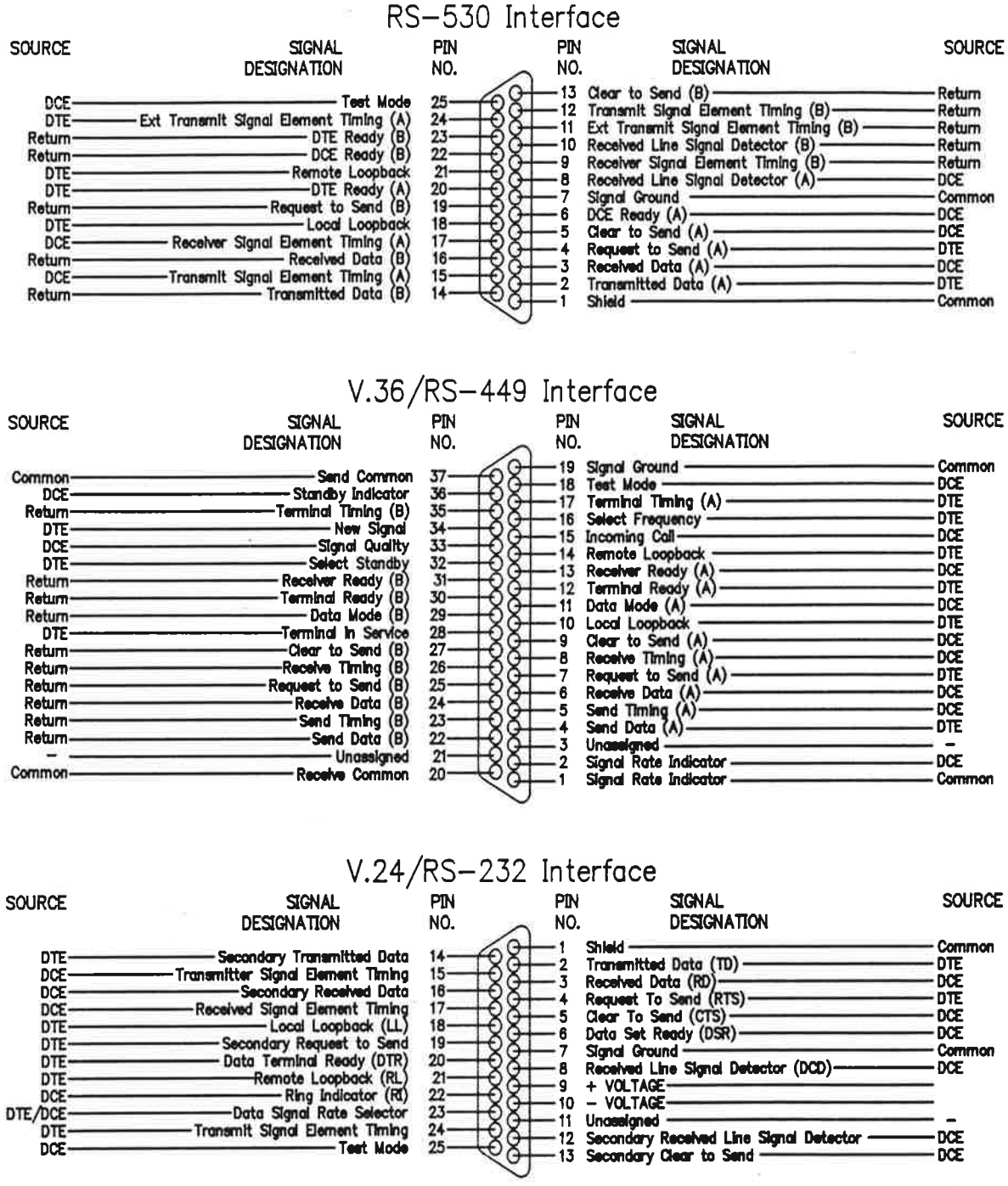
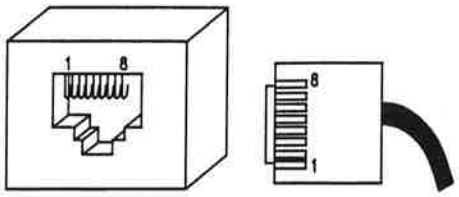


Figure 3-A HARDWARE INTERFACE CONNECTOR DIAGRAM

RJ-45 Pin Assignment

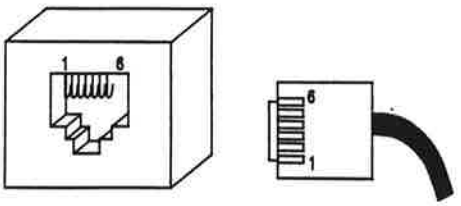


RJ-45 socket (female)
EXTERNAL view

RJ-45 plug (male)
Clip at rear

S-TAU, TAU-10 TAU-1 TRT TST	TMA	FLM-12 [RS-232]	STM's CMN-16 [RS-232]	Miniature Modems
8 NC	8 NC	8 CTS [5]	8 CTS [5]	8 NC
7 NC	7 Shield	7 Signal [7]	7 Signal [7]	7 NC
6 Transmit(orange)	6- 12VDC	6 DSR [6]	6 DTR [20]	6 Receive
5 Receive (green)	5- 12VDC	5 TX Data [2]	5 TX Data [2]	5 Transmit
4 Receive (red)	4 RS-485 -	4 DCD [8]	4 DCD [8]	4 Transmit
3 Transmit(black)	3 RS-485 +	3 RX Data [3]	3 RX Data [3]	3 Receive
2 NC	2 NC	2 RTS [4]	2 RTS [4]	2 Shield
1 NC	1 NC	1 +V Output [NC]	1 +V Output [1]	1 NC

RJ-11 Pin Assignment



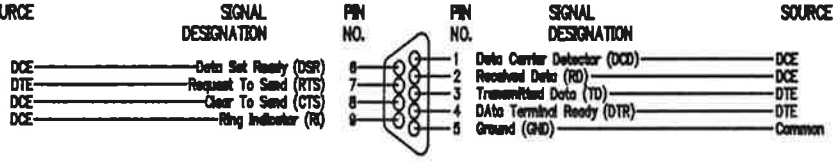
RJ-11 socket (female)
EXTERNAL view

RJ-11 plug (male)
Clip at rear

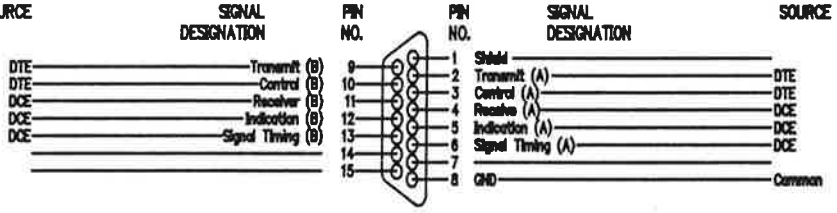
6 Shield
5 Receive
4 Transmit
3 Transmit
2 Receive
1 Shield

For SRM-3 SRM-4 SRM-5 SRM-6 SRM-8 ASM-11 CMH-16 miniature modems

V.24/RS-232 on a 9 Pin Connector



X.21 Interface



V.35 Interface

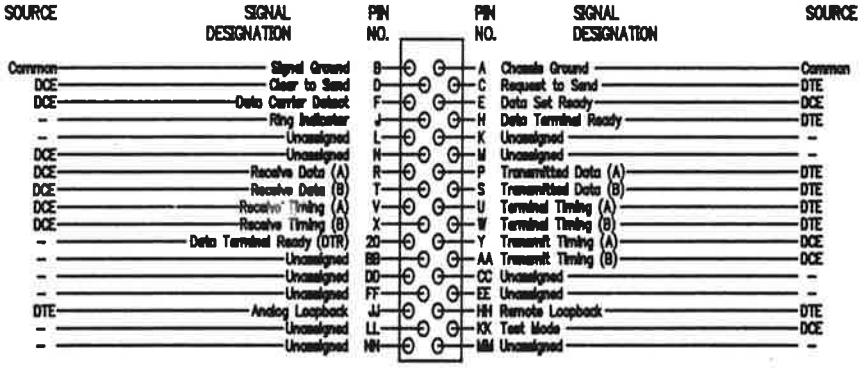


Figure 3-A HARDWARE INTERFACE CONNECTOR DIAGRAM (cont)

SECTION FOUR

4.0 SOFTWARE

NISE WEST is presently developing a prototype database to support SIIS using ORACLE7 Database Management System (DBMS). ORACLE7 is a major DBMS product and will provide the power and level of data integrity needed for the SIIS effort and is supported by a large number of different platforms. The prototype is being developed with the goal of satisfying as many immunization functions as possible, while retaining a simple user interface. Some of the features of the database are listed in the following paragraphs.

4.1 ORACLE7 Features

ORACLE7 is an open and portable software package that allows organizations to integrate their existing computer resources (both hardware and software) into flexible networks. ORACLE7 has the ability to merge different types of computers (WANG/DOS PCs/APPLE), operating systems (MS-DOS/OS2/ UNIX), networks (LAN/WAN), databases, and graphic user interfaces into an unified cooperative computing and information sharing network. ORACLE7 protects existing computer resource investments, while providing the flexibility of adding new technology in the future.

With ORACLE Open Gateway Technology, States with ORACLE can access most non-ORCALE data bases without modification. States without ORACLE can interface over standard ORACLE connecting services to

ORACLE databases. The ORACLE Open Gateway converts to and from ORACLE datatypes. ORACLE Open Gateway allows both ORACLE and non-ORACLE data sources to participate in transactions spanning multiple servers at multiple sites.

The Computer Security Act requires that all federal agencies protect their sensitive data with controlled access protection equivalent to Class C2-level. Class C2 is a controlled access protection of data through login procedures, auditing of security-relevant events, and resource isolation. ORACLE7 was designed to meet the National Computer Security Center (NCSC) Trusted Computer Systems Evaluation Criteria or the Orange Book Class C2-level security standard. This means that it can be used in Government/State installations requiring confidential access to the contents of a database.

Most States have a variety of local and wide area networks (LANs/WANs). Establishing a physical connection between any two computers requires that a common protocol (TCP/IP, AAC/LU6.2. SPX/IPX) be used. Networking applications evolved using computer connections for sharing information, thus implicitly limited them to communication over a single network protocol. ORACLE's Transparent Network Substrate uses the MultiProtocol Interchange to provide connectivity between multiple protocols into one heterogeneous network. ORCALE Protocol Adapters support ORACLE Application Networking by masking protocol differences.

Each protocol or computer-specific protocol implementation requires a unique Protocol Adapter. For example, unique Protocol Adapters exist for 3 COM TCP/IP, for MS-DOS, for FTP TCP/IP for MS-DOS, and Sun TCP/IP for SunOS.

4.2 Software Features

Character based interface: This allows providers with modems to access the system using any terminal emulation program, such as Procomm, Telix, Etc.

Form entry screens: All patient and immunization data is entered via screen forms. This provides a user friendly interface. It will require entry in some fields and provide browse lists where applicable to speed up entry and enforce data integrity.

Access levels: There will be three levels of access. Level one will have full access to all data. This would be the database administrator position, and would be at the state level. Level two users, typically providers, would be able to access immunization records for all patients, but would be limited on reports they could generate and records they could modify. Level three would be limited to checking if an individual is up to date without showing the patient's actual immunization history. This could possibly be a school.

The system is menu driven to enable the users to navigate through the various functions easily. The main menu gives the user the following options:

- **Individuals:** This selection is used to add new patients, find individuals and their status, and register immunizations.

- **Administration:** This option allows adding new users, vaccine inventory transaction options for both state and providers, and data input via the Birth Registry Interface.

- **Reports:** This allows generation of reports based on desired criteria. For providers, at present, it allows screen report generation for their own patients. State, or level one, users may generate reports on all patients based on desired criteria.

- **Help:** A help screen to provide on-line clarification of simple functions.

- **Quit - Log off the System:** One goal of the prototype database was to develop a core plan, and although it was developed using ORACLE, many of the higher level DBMS's such as SYBASE, INFORMIX, and INGRES have a high level of commonality. With slight modification the present schema could be used as a starting point for the other DBMS's and reduce development time. NISEWEST would be available to work with states who would be interested in pursuing this option.

4.2.1 Database Structure

The database structure for the Core Data Set is shown in the Tables 4-1 through 4-3.

TABLE 4-1

CORE DATA SET
INDIVIDUAL IDENTIFICATION

FIELD	TYPE	DESCRIPTION
PT-FIRST	Alpha (20)	patient's first name
PT-MIDDLE	Alpha (20)	patient's middle name
PT-LAST	Alpha (48)	patient's last name
PT-SSN	Alpha (9)	patient's Social Security no: 9 numeric characters
PT-BIRTH-DATE	Alpha (8)	patient's birth date format: YYYYMMDD
PT-BIRTH-FILE-NO	Alpha (16)	patient's birth registration number
PT-BIRTH-STATE	Alpha (3)	patient's State of birth
PT-MEDICAID-NO	Alpha (16)	patient's medicaid number
MOTHERS-FIRST	Alpha (20)	mother's first name
MOTHERS-MIDDLE	Alpha (20)	mother's middle name
MOTHERS-MAIDEN	Alpha (48)	mother's maiden name
MOTHERS-SSN	Alpha (9)	mother's Social Security no: 9 numeric characters
FATHERS-FIRST	Alpha (20)	father's first name
FATHERS-MIDDLE	Alpha (20)	father's middle name
FATHERS-LAST	Alpha (48)	father's last name
FATHERS-SSN	Alpha (9)	father's Social Security no: 9 numeric characters

SECTION FIVE

5.0 ELECTRONIC EQUIPMENT

5.1 Operational Electronic Equipment

The electronic equipment required for this project is listed in Table 5-1.

5.2 Electronic Test Equipment

Electronic test equipment used for maintenance of the equipment is listed in Table 5-2.

4.3 Internetworking Software

Additional required internetworking software will be determined after the state site survey.

4.4 Network Management Software

Required network management software will be determined after the state site survey.

4.5 Terminal Emulation Software

Required terminal emulation software will be determined after the state site survey.

4.6 Network Test Software

Required network test software will be determined after the state site survey.

4.7 Software Licensing Agreements

Software licensing agreements will be provided to all users for software obtained to support SIIS.

TABLE 4-2

CORE DATA SET
IMMUNIZATION TRANSACTION

FIELD	TYPE	DESCRIPTION
VACCINE-TYPE	Numeric (2)	code for vaccine type (see table below)
VACCINE-DOSE-NO	Numeric (2)	dose number for multiple dose series
VACCINATION-DATE	Alpha (8)	date of vaccination format: YYYYMMDD
VACCINE-LOT-NUMBER	Alpha (16)	lot number of vaccine
VACCINE-PROVIDER	Alpha (16)	REI facility ID

TABLE 4-3

CORE DATA SET
VACCINATION CODE CROSS REFERENCE

VACCINE TYPE	CODE	VACCINE TYPE	CODE
DTP	1	Monovalent Influenza	15
OPV	2	Trivalent Influenza	16
MMR	3	HbOC (Meningitis)	17
M/R	4	Rabies	18
Measles	5	BCG	19
Rubella	6	DTaP	20
Mumps	7	Varicella (Chicken Pox)	21
Hepatitis B	8	DTP-HbOC	22
Td (adult)	9	PRP-OMP	23
IPV	10	PRP-T	24
Pertussis (Whooping Cough)	11	Typhoid	25
Diphtheria	12	Cholera	26
TIG	13	DTP/ACTHib	27
ISG	14	DT Pediatric	28

TABLE 5-1

ELECTRONIC EQUIPMENT PROCUREMENT

ITEM NO.	NOMENCLATURE	TOTAL REQ'D	ON SITE	PROCUREMENT QUANTITY	REMARKS
1	File Server	*			
2	Router	*			
3	Modem	*			
4	Terminal Server	*			
5	Data Service Unit	*			
6	Bridges	*			
7	Hubs	*			
8	Sun Server	*			
9	FAX Server	*			
10	FAX	*			
11	Terminal Emulators	*			
12	MUXs	*			
13	REI Server	*			
14	PCs	*			
15	UPS & Mini-UPS	*			
16	Surge Protectors	*			
17	Power Filters	*			

* To be filled out during state site survey

TABLE 5-2

ELECTRONIC TEST EQUIPMENT REQUIREMENTS

ITEM NO.	FSCM/MODEL	TOTAL REQ'D	NOUN NAME	REMARKS
1	Data Breakout Boxes	*		
2	Cable Testers	*		
3	Digital Multimeters	*		
4	Earth Ground Tester	*		
5	Data Test Sets	*		
6	Transmission Line Tester	*		

* To be filled out during state site survey

SECTION SIX

6.0 NETWORK/SYSTEM CHECKOUT AND ACCEPTANCE

6.1 General Requirements

The network equipment and systems to be installed under this project will require checkout tests to ascertain that the network has been properly installed, will function adequately, and will meet the prescribed performance standards set forth in the appropriate instruction manuals. It is not intended for these tests to duplicate, substitute, or modify these tests.

Commercial Off the Shelf (COTS) equipment will normally have been tested to ensure that Electromagnetic Interference Compatibility tests, and Fire Safety tests have been successfully completed. The following certifications listed in Table 6-1, must be noted on the equipment case to verify conformance to the applicable commercial standards.

TABLE 6-1

EQUIPMENT/CERTIFICATION CROSS REFERENCE

EQUIPMENT	CERTIFICATION
UPS, Power Strips	Underwriter's Laboratories (UL 1449)
Modem	UL, Federal Communications Commission (FCC) Part 15 and Part 68
File Server	UL
Router	UL
Computers - 486 CPU - Monitors	UL UL, FCC Part 15
FAX	UL

6.2 Standards

Government and Commercial standards will be used wherever applicable as a basis for the design of the SIIS. Detailed checkout tests will be utilized to ensure that all network equipment is in optimum condition and that the system meets all operational requirements.

Individual equipment should be checked for UL and/or FCC certification. Additional information is detailed in Paragraph 3.1.

6.3 Individual Equipment Tests

Each network equipment installed during this SIIS project shall undergo tests to ensure that its actual performance conforms to its technical specifications. In general, the individual network equipment test will be as described in the applicable technical manual that accompanies the network equipment. Each test will be observed by a site representative. The site supervisor's signature will certify acceptance on the final sheet of the test document.

6.4 Overall System Tests

Overall system tests will be conducted to ensure optimum baseline system performance. System tests shall provide a record of performance. To allow for overall system uniformity and consistency, all incoming and outgoing signal levels will be set within the limits as prescribed by equipment technical manuals, instruction books, and other official documentation. The state site supervisor will observe the overall system test and sign his/her signature to the final system test document.

SECTION SEVEN

7.0 PHYSICAL PLANT

7.1 General Information

This section identifies known requirements for state site preparation. Physical location and equipment configuration shall be identified during the site survey. Table 7-1 lists typical equipment characteristics.

7.2 Power Requirements

Primary power required for the SIIS equipment is 120 Volt, 60 hertz single-phase. Uninterruptible Power Systems (UPS) or Mini-UPS for power loss protection to computer equipment will be identified during the state site survey. Additional items such as power filtering systems, power strips, surge and dip protectors will also be identified during the state site survey.

Requirements for additional circuit breakers or wall outlets will be forwarded to the state facility manager for action.

7.3 Telephone/Internet Service

Telephone connection points and Internet tie points will be identified during the state site survey. Requirements for telephone/Internet service will be forwarded to the state facility manager for action.

7.4 Environmental Control

Existing heating, ventilation, and air-conditioning (HVAC) units will be surveyed for adequacy. The network equipment must be in enclosed areas where the ambient temperature can be maintained between 40 and 110 degrees Fahrenheit. Requirements for additional environmental control equipment will be forwarded to the state facility manager for action.

7.5 Fire Protection

The State Immunization Information System (SIIS) will be protected in accordance with the existing state facility fire protection plan. Additional requirements identified during the state site survey will be forwarded to the state site facilities manager for action.

7.6 Grounding

All new network equipment installed for the SIIS will meet ANSI/NFPA 70 National Electrical Code standards. The facilities manager shall be responsible for action to ensure the standards are meet.

Table 7-1

EQUIPMENT CHARACTERISTICS TABULATION (PER UNIT BASIS)

ITEM NO.	EQUIPMENT NOMENCLATURE	EQUIPMENT DESCRIPTION	DIMENSIONS (INCHES)			WEIGHT (LBS)	QUANTITY			INPUT POWER (WATT)	VOLT/ CAT	HZ	PHASE	HEAT DISS BTU/HR	REMARKS
			HEIGHT	WIDTH	DEPTH		EXIST	NEW	TOTAL						

APPENDIX A

GLOSSARY OF

INTERNETWORKING TERMS

GLOSSARY OF INTERNETWORKING TERMS

Acoustic Coupler: a device that connects a computer modem or portable FAXs to the handset of a telephone. The telephone can be either a public, hotel or car type telephone.

Analog Links: are network links that are accessed by modems.

Application Layer: layer 7 of the OSI model; it defines protocols for user or application programs.

ASCII: American Standard Code for Information Interchange.

Backbone: a high-speed link joining several network bridges.

Bridge: a device that connects two networks of the same protocol together. A device operating at the OSI data link layer to connect local and wide area networks.

Bus Topology: all devices are connected to a central cable (the bus). Ethernet systems use bus topology.

Compression Program: replaces frequently occurring words or data with smaller, symbolic tokens that expand back to full words or data when the program is decompressed.

CSMA/CD: Carrier Sense Multiple Access/Collision Detection a network access method in which nodes contend for the right to send data.

CSU: Channel Service Unit (CSU) a communications device that connects an inhouse line to external digital link circuit. The CSU terminates the line and provides signal regeneration and remote testing.

Data Link layer 2 of the OSI model;it defines protocols **Layer:** governing data packetizing and transmission into and out of each node.

DCE: Data Communication Equipment (DCE) is a communication device that establishes, maintains, and terminates a session on a network; generally consists of modems and DSU/CSUs.

GLOSSARY OF INTERNETWORKING TERMS
(cont)

Dedicated Links: are networks that connected at all times. The customer is billed for the service whether it is used or not.

Digital Links: are network links that are accessed by DSUs and CSUs.

DNS: Domain Name System.

DSU: Data Service Unit (DSU) a communications device that connects an inhouse line to external digital link circuit. The DSU converts data into the required format.

DTE: Data Terminal Equipment (DTE) is a communication device that is the source or destination of signals on a network; generally consists of terminals or computers, bridges, and routers.

EBCDIC: Extended Binary Coded Decimal Interchange Code.

Emulation: the imitation of one device by another.

Ethernet: a 10 megabits per second baseband, CSMA/CD network originally designed by Xerox Corporation.

FAT: File Allocation Table (FAT) helps a file server keep track of where particular files are located.

FAX: Facsimile (FAX) machine is a device that sends and receives pictures and text over a telephone line.

File Server: a computer and storage device dedicated to storing network files. The computer maintains its own File Allocation Table (FAT) and provides files to the network nodes.

FTP: File Transfer Protocol.

GIF: Graphics Interchange Format.

Hub: a device that physically connects two or more cables together. The hub is the central point in a star physical topology.

GLOSSARY OF INTERNETWORKING TERMS
(cont)

Internet:	a national research-oriented network comprised of thousands of government and academic networks.
Internetworking:	to go between one network and another. A collection of two or more connected networks that may be dissimilar.
IP:	Internet Protocol governing packet forwarding.
LAN:	a local-area network (LAN) is a group of computers linked together in a close geographic area (in the same building).
Modem:	a device converts digital pulses into frequencies within the audio range of the telephone and converts them back into pulses at the receiving side.
MUX:	Multiplexor (MUX) is a device that merges several low-speed transmissions into one high-speed transmission.
Network: Architecture	the design of a communications system which includes hardware, access methods, software, and protocols used.
Network:	a group of two or more computer systems linked together.
Network Layer:	layer 3 of the OSI model; it defines protocols governing data routing.
Node:	an individual PCs on a Local Area Network.
OSI:	Open Systems Interconnection (OSI) a seven-layer protocol model designed for data communications.
Packet:	a collection of bits comprising data and control information formatted for transmission from one node to another.
Packet Switching:	a data transmission method that routes packets along the most efficient path and allows a communications channel to be shared by multiple connections.
Physical Layer:	layer 1 of the OSI model; it details protocols governing transmission media and signals.

GLOSSARY OF INTERNETWORKING TERMS
(cont)

Presentation Layer:	layer 6 of the OSI model; it defines protocols governing data formats and conversions.
Protocol:	an agreed-upon format for transmitting data between devices. A set of rules and regulations that govern the transmitting and receiving of data.
Ring Topology:	all devices are connected to one another in the shape of a closed loop or ring.
Router:	a device that selects an appropriate travel path and routes a message accordingly. A device that links two networks that are running different protocols.
Session Layer:	layer 5 of the OSI model; it defines protocols governing communication between applications.
SNA:	Systems Network Architecture (SNA) IBMs protocols governing mainframe communications.
Star Topology:	all devices are connected to a central hub.
Switched Links:	are networks that are established between any two points and incur cost only while established.
TCP:	Transmission Control Protocol governing sequenced data.
Terminal:	a device that attaches to a multi-user computer. A terminal has a keyboard for entering information into the computer and a monitor for displaying information from the computer. A terminal has no computing power of it own.
Terminal Emulator:	a device that emulates a particular type of terminal.
Terminal Server:	a terminal in a network that is shared by multiple users.
Topology:	the physical arrangement or shape of a local-area network. There are three principal topologies used for LANs, the bus, ring, and star.
Transport Layer:	layer 4 of the OSI model; it defines protocols governing message structure and some error checking.

WAN: a wide-area network (WAN) is a group of computers linked together in a wide area and are connected by telephone lines or radio waves.

APPENDIX B

ACRONYMS AND ABBREVIATIONS

ACRONYMS AND ABBREVIATIONS

ADP	Automatic Data Processing
ANSI	American National Standards Institute
ARPA	Advanced Research Project Agency
CDC	Centers for Disease Control and Prevention
COTS	Commercial Off The Shelf
DBMS	Database Management System
DSU	Data Service Unit
DT	Diphtheria and Tetanus
DTP	Diphtheria, Tetanus Toxoids, Pertussis Vaccine
FAX	Facsimile
FCC	Federal Communications Commission
FTP	File Transfer Protocol
HbOC	Conjugate Form of Meningitis Vaccine
HEP	Hepatitis
Hib	Haemophilus Influenza Type B
Hrs	Hours
HVAC	Heating, Ventilation and Air Conditioning Unit
IP	Internet Protocol
IPV	Inactivated (Killed) Polio Vaccine
ISE	In-Service Engineering
kb	kilo byte
LAN	Local Area Network

ACRONYMS AND ABBREVIATIONS
(cont)

Mb	Mega byte
MIL	Military
MMR	Measles, Mumps, and Rubella Virus Vaccine Live
MS-DOS	Micro Soft - Disk Operating System
MUX	Multiplexer
NASA	National Aeronautical Space Administration
NCSC	National Computer Security Center
NIP	National Immunization Program
NSF	National Science Foundation
NSFNET	National Science Foundation Network
NT	New Technology
OPV	Oral Polio Virus Vaccine Live
OSI	Open System Interconnection
PC	Personal Computer
PRP	Purified Polysaccharide Form of Vaccine
REI	Record Exchange Interface
RMS	Record Management System
sec	Second
SIIS	State Immunization Information System
STD	Standard
SunOS	Sun Operating System
TCP	Transmission Control Protocol

ACRONYMS AND ABBREVIATIONS
(cont)

Td	Tetanus and Diphtheria Toxoids
TIG	Tetanus Immune Globulin
TELCO	Telephone Company
UL	Underwriters Laboratory
UPS	Uninterruptible Power System
WAN	Wide Area Network

APPENDIX C

NATIONAL IMMUNIZATION PROGRAM (NIP)

AND NISE WEST

POINTS OF CONTACT

NATIONAL IMMUNIZATION PROGRAM (NIP) AND NISE WEST POINTS OF CONTACT

NAME	TITLE	ADDRESS	PHONE/FAX/EMAIL NUMBERS
Donald L. Eddins	Director Data Management Division National Immunization Program	Centers for Disease Control and Prevention National Immunization Program Data Management Division 1600 Clifton Rd., MS E-62 Atlanta, Georgia 30333	Tel: (404) 639-8256 Email: DLE1@nip1.em.cdc.gov
Mark Schrader	Deputy Director Data Management Division National Immunization Program	Centers for Disease Control and Prevention National Immunization Program Data Management Division 1600 Clifton Rd., MS E-62 Atlanta, Georgia 30333	Tel: (404) 639-8209 Email: MVS3@nip1.em.cdc.gov
George Seastrom	Public Health Advisor Data Management Division National Immunization Program	Centers for Disease Control and Prevention National Immunization Program Data Management Division 1600 Clifton Rd., MS E-62 Atlanta, Georgia 30333	Tel: (404) 639-8245 Email: GES1@nip1.em.cdc.gov
Robert P. Cruz	Department Director Terrestrial Communications NISE West Code 210	NISE West Code 210 Terrestrial Communications 4297 Pacific Highway San Diego, California 92186-5137	Tel: (619) 524-2851 FAX: (619) 524-2820 Email: cruzrp@nisewest.nosc.mil
Milton Martinez	Division Head Telecommunications and Engineering Division NISE West Code 213	NISE West Code 213 Telecommunications and Engineering Division 4297 Pacific Highway San Diego, California 92186-5137	Tel: (619) 524-3658 FAX: (619) 524-3148 Email: martinezm@nisewest.nosc.mil
Gregory Lee	Field Support Manager Telecommunications and Engineering Division NISE West Code 213	NISE West Code 213 Telecommunications and Engineering Division 4297 Pacific Highway San Diego, California 92186-5137	Tel: (619) 524-2700 FAX: (619) 524-3148 Email: leegl@nisewest.nosc.mil
David Talley	Program Manager Telecommunications and Engineering Division NISE West Code 213	NISE West Code 213 Telecommunications and Engineering Division 4297 Pacific Highway San Diego, California 92186-5137	Tel: (619) 524-2704 FAX: (619) 524-3148 Email: talleydl@nisewest.nosc.mil

APPENDIX D

NISE WEST/NATIONAL IMMUNIZATION PROGRAM (NIP) CONSULTANTS/PROJECT OFFICER REGIONAL ASSIGNMENTS

NISE WEST/NATIONAL IMMUNIZATION PROGRAM (NIP)
CONSULTANTS/PROJECT OFFICER REGIONAL ASSIGNMENTS

REGION	STATES	NISE WEST TECHNICAL COORDINATOR	NIP CONSULTANT		
			Name	Phone Number	Internet Email
I	Connecticut Maine Massachusetts New Hampshire Rhode Island Vermont	William Jones (619) 524-2162 Internet Email: joneswh@nisewest.nosc.mil	1. Joe Beaver 2. Harry McKnight 3. Glen Koops	(404) 639-8209 (404) 639-8209 (404) 639-8209	JHB5@nip1.em.cdc.gov HLM4@nip1.em.cdc.gov GAK3@nip1.em.cdc.gov
II	New Jersey New York State New York City Puerto Rico Virgin Island	Rene Cruz (619) 524-3147 Internet Email: cruzra@nisewest.nosc.mil	1. Rick Nelson 2. Harry McKnight	(404) 639-8209 (404) 639-8209	MRN2@nip1.em.cdc.gov HLM4@nip1.em.cdc.gov
III	Delaware Maryland Pennsylvania Virginia Washington DC West Virginia	William Jones (619) 524-2162 Internet Email: joneswh@nisewest.nosc.mil	1. Lewis Anderson 2. Harry McKnight 3. Valerie Kokor	(404) 639-8209 (404) 639-8209 (404) 639-8209	LSA1@nip1.em.cdc.gov HLM4@nip1.em.cdc.gov VAK1@nip1.em.cdc.gov
IV	Alabama Florida Georgia Kentucky Mississippi North Carolina South Carolina Tennessee	Larry White (619) 524-2575 Internet Email: whitel@nisewest.nosc.mil	1. Ken Allman 2. Gary Rhyne	(404) 639-8209 (404) 639-8209	KCA1@nip1.em.cdc.gov GJR1@nip1.em.cdc.gov
V	Chicago Illinois Indiana Michigan Minnesota Ohio Wisconsin	Greg Lee (619) 524-2375 Internet Email: leegl@nisewest.nosc.mil	1. Gary Rhyne 2. Ken Allman 3. Ken Sharp	(404) 639-8209 (404) 639-8209 (404) 639-8209	GJR1@nip1.em.cdc.gov KCA1@nip1.em.cdc.gov KLS2@nip1.em.cdc.gov

NISE WEST/NATIONAL IMMUNIZATION PROGRAM (NIP) CONSULTANTS/PROJECT OFFICER REGIONAL ASSIGNMENTS (cont)

REGION	STATES	NISE WEST TECHNICAL COORDINATOR	NIP CONSULTANT		
			Name	Phone Number	Internet Email
VI	Arkansas Louisiana New Mexico Oklahoma Texas Houston San Antonio	Willie Levett (619) 524-2014 Internet Email: levettwb@nisewest.nosc.mil	1. Valerie Kokor 2. Glen Koops 3. Rick Nelson	(404) 639-8209 (404) 639-8209 (404) 639-8209	VAK1@nip1.em.cdc.gov GAK3@nip1.em.cdc.gov MRN2@nip1.em.cdc.gov
VII	Iowa Kansas Missouri Nebraska	Dave Talley (619) 524-2704 Internet Email: talleydl@nisewest.nosc.mil	1. Ken Sharp 2. Valerie Kokor 3. Ken Allman	(404) 639-8209 (404) 639-8209 (404) 639-8209	KLS2@nip1.em.cdc.gov VAK1@nip1.em.cdc.gov KCA1@nip1.em.cdc.gov
VIII	Colorado Montana North Dakota South Dakota Utah Wyoming	Julian Evola (619) 524-2001 Internet Email: evolaj@nisewest.nosc.mil	1. Harry McKnight 2. Ken Sharp 3. Lewis Anderson	(404) 639-8209 (404) 639-8209 (404) 639-8209	HLM4@nip1.em.cdc.gov KLS2@nip1.em.cdc.gov LSA1@nip1.em.cdc.gov
IX	American Samoa Arizona California Guam Hawaii Marshall Island Micronesia North Merianas Palau	Julian Evola (619) 524-2001 Internet Email: evolaj@nisewest.nosc.mil	1. Glen Koops 2. Lewis Anderson 3. Gary Rhyne	(404) 639-8209 (404) 639-8209 (404) 639-8209	GAK3@nip1.em.cdc.gov LSA1@nip1.em.cdc.gov GJR1@nip1.em.cdc.gov
X	Alaska Idaho Oregon Washington	Greg Lee (619) 524 -2375 Internet Email: leegl@nisewest.nosc.mil	1. Ken Sharp 2. Valerie Kokor 3. Ken Allman	(404) 639-8209 (404) 639-8209 (404) 639-8209	KLS2@nip1.em.cdc.gov VAK1@nip1.em.cdc.gov KCA1@nip1.em.cdc.gov