

1/19

**CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES
LOCAL AREA NETWORK (LAN)
SECURITY PLAN**

Prepared for

**Nuclear Regulatory Commission
Contract NRC-02-93-005**

Prepared by

**Alfred L. Johnson
Robert L. Marshall
Rawley D. Johnson**

**Center for Nuclear Waste Regulatory Analyses
San Antonio, Texas**

January 1995

2/19

CONTENTS

Section	Page
FIGURES	iii
TABLES	iv
ACKNOWLEDGMENTS	v
1 SYSTEM IDENTIFICATION	1-1
1.1 RESPONSIBLE ORGANIZATION	1-1
1.2 SYSTEM NAME/TITLE	1-1
1.3 SYSTEM CATEGORY	1-1
1.4 SYSTEM OPERATIONAL STATUS—OPERATIONAL/ UNDERGOING MAJOR MODIFICATION	1-1
1.5 GENERAL DESCRIPTION/PURPOSE	1-1
1.6 SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS	1-2
1.7 INFORMATION CONTACT(S)	1-2
2 SENSITIVITY OF INFORMATION HANDLED	2-1
2.1 APPLICABLE LAWS OR REGULATIONS AFFECTING THE SYSTEM	2-1
2.2 GENERAL DESCRIPTION OF INFORMATION SENSITIVITY	2-1
3 SYSTEM SECURITY MEASURES	3-1
3.1 RISK ASSESSMENT AND MANAGEMENT	3-1
3.2 APPLICABLE GUIDANCE (AGENCY POLICY, GUIDELINES)	3-2
3.3 SECURITY CONTROL MEASURES	3-2
3.4 SECURITY CONTROL MEASURES STATUS	3-2
3.5 SECURITY CONTROL MEASURES FOR MAJOR APPLICATIONS	3-3
3.6 SECURITY CONTROL MEASURES FOR GENERAL SUPPORT SYSTEMS	3-3
3.6.1 Management Controls—In Place and Planned	3-3
3.6.2 Acquisition/Development/Installation Controls—In Place and Planned	3-3
3.6.3 Operational Controls—In Place	3-4
3.6.4 Security Awareness and Training—In Place and Planned	3-5
3.6.5 Technical Controls—In Place and Planned	3-6
3.6.6 Controls Over the Security of Applications—In Place and Planned	3-7
4 REFERENCES	4-1

FIGURES

Figure		Page
1-1	Current Center for Nuclear Waste Regulatory Analyses (CNWRA) San Antonio and Washington Technical Support Office (WTSO) network topology	1-4
1-2	Planned Center for Nuclear Waste Regulatory Analyses (CNWRA) San Antonio and Washington Technical Support Office (WTSO) network topology	1-5

4/19

TABLES

Table	-	Page
3-1	Center Nuclear Waste Regulatory Analyses (CNWRA) local area network (LAN) risk factors	3-1

ACKNOWLEDGMENTS

This report was prepared to document work performed by the Center for Nuclear Waste Regulatory Analyses (CNWRA) for the Nuclear Regulatory Commission (NRC) under Contract No. NRC-02-93-005. This report was formatted in accordance with NUREG/BR-0166 (Nuclear Regulatory Commission) to comply with OMB Bulletin No. 90-08 (Office of Management and Budget, 1990). The activities reported here were performed on behalf of the NRC Office of Nuclear Material Safety and Safeguards (NMSS), Division of Waste Management (DWM). The report is an independent product of the CNWRA and does not necessarily reflect the views or regulatory position of the NRC.

The following trademarks are used in this report:

- OS/2 is a trademark of the International Business Machine (IBM) Corporation
- Macintosh is a trademark of Apple Corporation
- UNIX is a registered trademark of Unix System Laboratories, Inc.
- SPARCstation is a trademark of SPARC International, Inc.
- Wellfleet and Synoptics are trademarks of Bay Networks
- SGI is a trademark of Silicon Graphics, Inc.
- Ethernet is a trademark of Xerox Corporation
- VAX is a trademark of Digital Equipment Corporation

6/19

1 SYSTEM IDENTIFICATION

1.1 RESPONSIBLE ORGANIZATION

Center for Nuclear Waste Regulatory Analyses (CNWRA)

1.2 SYSTEM NAME/TITLE

CNWRA Local Area Network (LAN)

1.3 SYSTEM CATEGORY

General Support System

1.4 SYSTEM OPERATIONAL STATUS-OPERATIONAL/UNDERGOING MAJOR MODIFICATION

The CNWRA LAN became operational in October 1993. Following discussions of security requirements with the Nuclear Regulatory Commission (NRC) during March-September 1994 and approval of the CNWRA Network Security Proposal (Marshall and Johnson, 1994) by Information Resource Management (IRM) on November 18, 1994, a major modification to the LAN was begun to implement the firewall. It is projected that this modification will be completed in April 1995. Any references to the current topology reflect the LAN configuration as of the date of this security plan. Any references to the planned topology will reflect the LAN configuration at the completion of the approved firewall implementation in April 1995.

1.5 GENERAL DESCRIPTION/PURPOSE

The purpose of the CNWRA LAN is to support regulatory, technical, and institutional analyses in accordance with the Nuclear Waste Policy Act (NWPA), as amended. Under the NWPA, the Division of Waste Management (DWM) of the NRC will regulate the U.S. Department of Energy (DOE) in its design, construction, operation, and closure of a high-level nuclear waste (HLW) repository. The CNWRA LAN is implemented and supported by the CNWRA in San Antonio, Texas.

The CNWRA LAN consists of approximately seven UNIX servers on an ethernet LAN with approximately 80 OS/2 personal computers (PCs), 25 Sun workstations, and 10 Macintosh systems. The CNWRA organization is part of Southwest Research Institute (SwRI) and is connected to the SwRI LAN via a router. The CNWRA staff in San Antonio, Texas, are connected through a wide area network consisting of routers and a fractional T1 leased line to the NRC at Two White Flint North in Rockville, Maryland, and the CNWRA Washington Technical Support Office (WTSO) in Arlington, Virginia.

The CNWRA LAN provides support services for Office Automation applications (including financial and personnel applications), Scientific/Engineering Computing applications, and a Regulatory Analysis applications involving predecisional data [the Regulatory Program Database (RPD)/Technical Reference Document Database System (TDOCS)] (DeWispelare et.al., 1994). The security requirements

7/19

for all of these applications were examined to determine those needed for the CNWRA LAN. The RPD/TDOCS system implements additional, specific controls and is covered in a separate security plan.

1.6 SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

The current CNWRA LAN topology is shown in Figure 1-1. The San Antonio CNWRA office is located in three separate buildings. Buildings 51 and 57 are served with a single ethernet segment; Building 189 is served by two Synoptics 3000 series concentrators. These buildings are connected by one of the SwRI Cisco routers. The Wellfleet router connecting the San Antonio network to the NRC and to the CNWRA WTSO in Crystal City, Virginia, is located on the first floor in Building 189.

The planned network topology described in this report is shown in Figure 1-2 and includes a CNWRA "firewall" system equivalent to the NRC firewall system. A new ethernet segment, the perimeter net, connects to the SwRI Cisco router through a new Cisco router (external router) that provides the first line of defense from the Internet. This perimeter net (also known as the demilitarized zone, or DMZ) has its own distinct network number (subnet). A packet filter gateway connects the perimeter net to the internal CNWRA network. A second Cisco router (internal router) has been added to the internal network to route between the three buildings. A bastion host is located on the perimeter net to provide proxy services for Simple Mail Transfer Protocol, Domain Name Service, and Network News Transfer Protocol, as well as to perform monitoring tasks for the perimeter net. This design is detailed in the approved CNWRA Network Security Proposal (Marshall and Johnson, 1994).

The CNWRA LAN has two interface points. The first connects the CNWRA LAN to the SwRI backbone at the CNWRA external router. Everything on the SwRI side is considered suspect. The second interface point connects the CNWRA LAN to the NRC Agency Wide area Network (AWN). The NRC provides Wellfleet routers and communication lines to connect the San Antonio and WTSO portions of the CNWRA LAN to the NRC AWN. Everything on the NRC side is considered trusted.

All of the San Antonio portion of the LAN is located on the SwRI campus, which is security patrolled. Buildings 51, 57, and 189 are all locked and patrolled after work hours. Key security equipment, including phone closets, routers, firewall equipment, fiber-optic lines, etc., are stored in locked offices or closets. Access is restricted to SwRI telecommunications personnel and CNWRA Information Management System (IMS) staff. The WTSO is locked 24 hours a day.

1.7 INFORMATION CONTACT(S)

Rawley D. Johnson (CNWRA)
Director—IMS
(210) 522-5153

Robert L. Marshall (CNWRA)
Database Administrator—IMS
(210) 522-5248

8/
19

Marvin Marshall [SwRI Computer and Telecommunications Center (CTC)]
Director—CTC
(210) 522-2298

George Stevenson (SwRI Security)
Manager—Facility Security Officer
(210) 522-5642

14

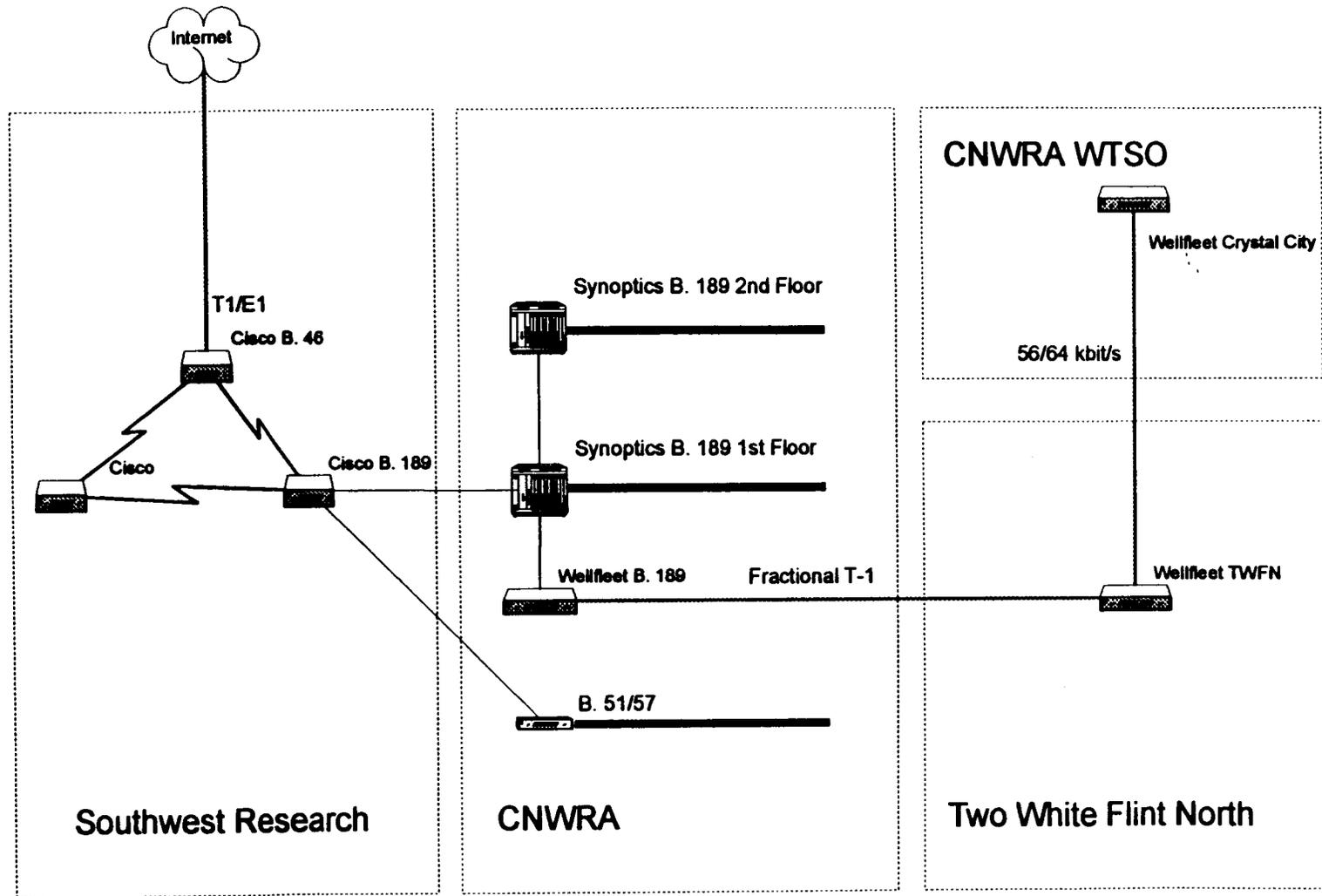


Figure 1-1. Current Center for Nuclear Waste Regulatory Analyses (CNWRA) San Antonio and Washington Technical Support Office (WTSO) network topology

b1/b

1-5

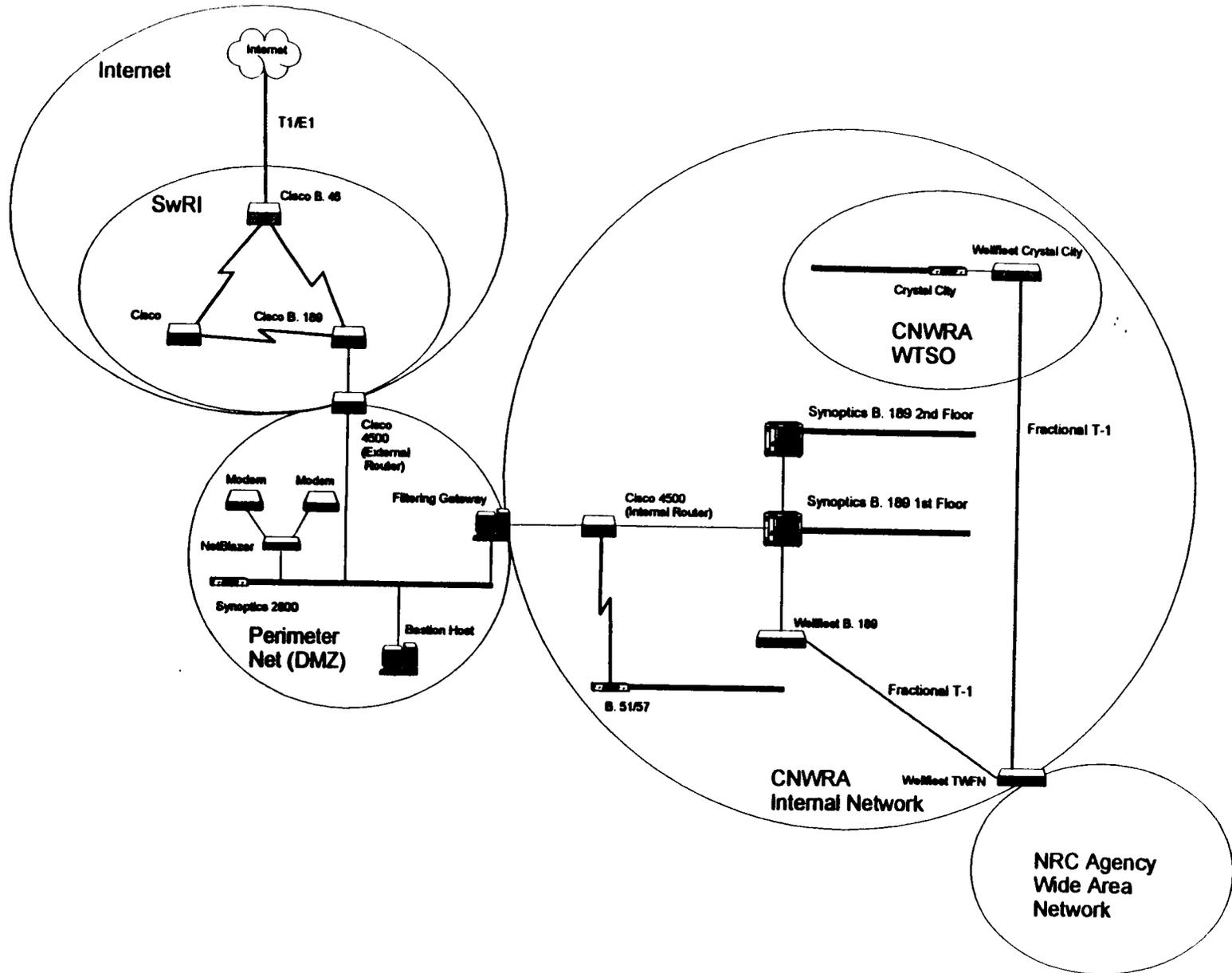


Figure 1-2. Planned Center for Nuclear Waste Regulatory Analyses (CNWRA) San Antonio and Washington Technical Support Office (WTSO) network topology

b1/01

11/19

2 SENSITIVITY OF INFORMATION HANDLED

2.1 APPLICABLE LAWS OR REGULATIONS AFFECTING THE SYSTEM

Information maintained and transmitted by this LAN is covered by the Privacy Act of 1974 (5 U.S.C. 552a), 10 CFR Part 2 (Nuclear Regulatory Commission, 1994), and 10 CFR Part 9 (Nuclear Regulatory Commission, 1994). Any attempt to access the information in an unauthorized manner or damage the data in transit may be covered by the Computer Crimes Act of 1994 (Public Law 103-322).

2.2 GENERAL DESCRIPTION OF INFORMATION SENSITIVITY

(i) Confidentiality—High

The LAN stores and transmits predecisional information used by the DWM in implementing its responsibilities under the NWPA. This information is used to determine how the NRC might evaluate the DOE license for a high-level waste repository. CNWRA personnel and financial data is also produced and stored on the LAN. The disclosure of personnel data might be a violation of the Privacy Act of 1974.

(ii) Integrity—High

The CNWRA LAN is used to produce, store, and manage scientific and engineering data. These data are used to support the CNWRA key mission to provide scientific analysis to the NRC. Modification of such data could lead to repeating expensive experiments (due to lost or corrupted data) or to erroneous conclusions being made (due to erroneous data).

(iii) Availability—High

The failure of the LAN and/or loss of data stored on the LAN would prevent the CNWRA from performing day-to-day activities and jeopardize the NRC HLW program.

12/19

3 SYSTEM SECURITY MEASURES

3.1 RISK ASSESSMENT AND MANAGEMENT

Risk analysis tools have been used to perform a portion of a risk analysis of the CNWRA LAN. CNWRA IMS staff members have used public domain software such as "crack" to assess the risk of vulnerability of passwords on the CNWRA LAN. Identified risk factors, their relation to information sensitivity, preventive mechanisms, and the relative magnitude of the risk, as determined by CNWRA staff, is listed in Table 3-1.

Table 3-1. Center for Nuclear Waste Regulatory Analyses (CNWRA) local area network (LAN) risk factors

Risk	Risk Factor	Preventive Mechanism	Magnitude of Risk
Disclosure	Unauthorized access via Internet	CNWRA Firewall (CNWRA Network, Security Proposal, Sept. 1994)	Medium
	Unauthorized access via modem	Removal of individual modems/Modem Pool	Low
	Unintentional or intentional transfer of sensitive information	Personnel screening, Operational policies, User education	High
Data Modification	Unauthorized access via Internet	CNWRA Firewall	Medium
	Unauthorized access via modem	Removal of individual modems/Modem Pool	Low
	Unintentional or intentional modification of sensitive information	Personnel screening, Operational policies, User education	High
Unavailability	Disaster (e.g. fire)	Backup/Off-site storage	Low
	Denial of service attacks	CNWRA Firewall	Low

The following items are risks that CNWRA has identified as a result of this informal risk assessment:

- One system left unsecure on the LAN could put all the rest at risk. The security plan should protect all of the CNWRA computer systems and network assets. The information to be protected is not limited to a few computers.
- There is a risk that the CNWRA LAN computers are exposed to compromise by creative UNIX and PC hackers with the competence to build viruses or dictionary-based password crackers.
- There is a security risk from known operating system software deficiencies.
- There is a security risk in implicitly allowing external computers outside the CNWRA LAN to have uncontrolled access to computers on the CNWRA LAN.
- The use of unsecured network applications is a risk. The CNWRA often uses Internet services through applications that provide for the transfer of data containing computer identification information that is essential to that computer's security.
- The procedures for assignment and maintenance of passwords on CNWRA LAN servers is at risk if hackers can utilize "password cracking" tools to get access to those passwords.

3.2 APPLICABLE GUIDANCE (AGENCY POLICY, GUIDELINES)

The following guidelines were used in the preparation of this security plan:

- OMB Bulletin No. 90-08—Guidance for Preparation of Security Plan for Federal Computer Systems that Contain Sensitive Information
- NUREG/BR-0166—Instructions for Preparing Security Plans for Local Area Networks in Compliance with OMB Bulletin No. 90-08

3.3 SECURITY CONTROL MEASURES

Security control measures included in this plan have been addressed from the perspective of management and CNWRA staff directly responsible for the administration of the security for the LAN.

3.4 SECURITY CONTROL MEASURES STATUS

Specific management, operational, and technical measures that are either in place as of January 1, 1995, planned as of April 1, 1995, or in place and planned, are described in Section 3.6 of this plan.

3.5 SECURITY CONTROL MEASURES FOR MAJOR APPLICATIONS

Not applicable. The system is a general support system (a system used by many users in different locations within the same organization). The security control measures are defined in the following section.

3.6 SECURITY CONTROL MEASURES FOR GENERAL SUPPORT SYSTEMS

3.6.1 Management Controls—In Place and Planned

(i) Assignment of Security Responsibility—In Place

The duties of system security officer have been assigned to the following individual:

Robert Marshall (CNWRA)
Database Administrator
(210) 522-5248

(ii) Risk Analysis—In Place and Planned

The risk analysis that was previously performed (Section 3.1) addressed the need to secure the entire CNWRA LAN. This analysis took into consideration securing the overall ethernet network at a high level by implementing a firewall system as well as securing individual computers at the lowest level. The CNWRA plans to utilize several public domain software packages (e.g., COPS, TIGER, and TRIPWIRE) on servers and individual workstations to assess potential risks in the operating system configuration.

(iii) Personnel Screening—In Place and Planned

Personnel screening under the CNWRA Quality Assurance (QA) program is performed and documented annually as described in AP-001 Evaluation of Potential Conflict of Interest (Center for Nuclear Waste Regulatory Analyses, 1994a), QAP-005 Quality Indoctrination and Training (Center for Nuclear Waste Regulatory Analyses, 1994b), and QAP-007 Employment Procedures for Professional Staff (Center for Nuclear Waste Regulatory Analyses, 1990). Every employee or consultant must be screened before they are allowed access to sensitive information. Any potential consultant who wishes to have remote access to CNWRA LAN computers must first be approved by the NRC DWM and IRM.

3.6.2 Acquisition/Development/Installation Controls—In Place and Planned

(i) Acquisition Specifications—Planned

Some of the computers that the CNWRA has purchased (i.e., UNIX workstations), to date, have inherent security features that enable some level of security, although not at the highest level, and will be enabled. With the approval of the CNWRA Network Security Proposal, the CNWRA is in the process of acquiring specific computer hardware

(e.g., Cisco routers), and Sun workstations that will be configured specifically for securing the CNWRA LAN. The plan is to secure individual computers by installing and configuring public domain software as well as enabling the security features that are inherent in the operating system.

(ii) **Accreditation/Certification—In Place and Planned**

An internal QA audit is performed annually of all CNWRA computer systems by the SwRI QA staff, with observers from the NRC DWM staff. This audit is planned in the next QA milestone and a certification of the CNWRA firewall is scheduled for May 1995.

3.6.3 Operational Controls—In Place

(i) **Physical and Environmental Protection—In Place**

SwRI entrance is manned by security guards that check all unauthorized vehicles. Each building has locks to secure it and is locked by the guards before and after hours. Guards make periodic checks of each building. At CNWRA, each office has a lock on the door and the employee is provided with a key. Computer labs that have more than one computer also have locks on the door. The whole building has smoke alarms and fire extinguishers are installed in the event of a fire. Each computer is provided with a surge protector and every Sun workstation and major server also has an uninterruptable power supply in the event of loss of power.

(ii) **Production, Input/Output (I/O) Controls—In Place**

Most archival media are handled by the System Administrator. The tape media are labeled appropriately and stored in various locations depending upon frequency of use. Short-term archives may be located by the computer it resided on, and long-term archives may reside in the secure, fire-proof vault, locked in a room assigned to QA. Paper printouts are produced at the CNWRA buildings and all retained paper output is controlled by CNWRA administrative procedures. All waste paper is recycled by a bonded third party. All of these materials may contain sensitive information and therefore all materials are treated as sensitive.

(iii) **Emergency, Backup, and Contingency Planning—In Place and Planned**

All major servers on the LAN are backed up daily. Incremental and full backups are performed in the event of an emergency or disaster. These disaster recovery tapes are sent offsite once a month for storage. Only one copy of these tapes currently exists offsite. In the event of computer hardware failure, these tapes can be restored to another leased computer. CNWRA plans to acquire and implement a centralized network backup solution for the various computers. This backup solution would perform centralized unattended backups in the off hours over the network for all the CNWRA computers, assuming that the software handles all the computer clients that the CNWRA has implemented. At most, there would be only two backup servers that would handle all of the computers. This solution will also provide the capability to make a copy of the disaster recovery tapes that are being sent offsite, so that a copy could be retained in the

16/19

CNWRA fire-proof vault as additional insurance. This automated process also provides for manual intervention to back up data to tape.

(iv) **Audit and Variance Detection—In Place and Planned**

Currently, variance detection in the form of virus scanning is performed on those computers that provide this capability. By using a virus-scanning software package, the CNWRA can detect and clean computer viruses introduced by a foreign source. This has been done, as some CNWRA computers were infected with the "Jerusalem" virus. The CNWRA plans to continue to use this virus-scanning software in addition to some other means for auditing. The CNWRA currently utilizes and will expand on using network monitoring software from Sun Microsystems, Inc. to audit utilization of servers and detect abnormal operating conditions on the network. This will enable staff to take appropriate action without delay. In addition, the CNWRA will implement logging of firewall activity and automatic notification of intrusion and abnormal remote login attempts.

(v) **Hardware and System Maintenance Controls—Planned**

System maintenance is performed by CNWRA IMS staff who hold administrative passwords for major servers. Primarily, the servers, multi-user workstations, and the computers that are directly related to the firewall each have a logbook that is maintained whenever hardware or software is installed or reconfigured. In addition, the CNWRA has recently defined approved and nonapproved software and operating systems for use by staff and uses this as a means of controlling proliferation of unauthorized software. Usually, the IMS staff will test hardware and software within the IMS element before making it available to other staff.

(vi) **Documentation—In Place and Planned**

The CNWRA Network Security Proposal, prepared by CNWRA IMS staff and submitted to the NRC describes the CNWRA LAN and documents the hardware and software that are in place and planned in securing the CNWRA LAN. Detailed policy and procedures are forthcoming while the implementation of the firewall takes place. In this plan are detailed diagrams of the network topology before and after the implementation of the firewall, just as are detailed in Section 1 of this document.

3.6.4 Security Awareness and Training—In Place and Planned

(i) **Security Awareness and Training Measures—In Place and Planned**

The CNWRA IMS staff have developed a CNWRA Resource Guide and have made users aware (Center for Nuclear Waste Regulatory Analyses, 1994c) of good computer practices that they should follow relating to security, for example, selecting passwords that are less likely to be cracked, using screen locks, or not sharing passwords. More recently, a CNWRA IMS seminar was held that discussed network security and good use practices for the Internet with regards to the future implementation of the CNWRA firewall. All users of this secure network will have access to documentation in the form of a Resource Guide that details the policies and procedures. Those employees

responsible for the design, management, implementation, and maintenance of the secured network currently know and will know future responsibilities as the firewall is implemented. These individuals will receive on-the-job training and attend training courses as the need develops. These individuals currently do and will continue to meet weekly to discuss any computer-related issues, whether or not they are security related.

3.6.5 Technical Controls—In Place and Planned

(i) User Identification and Authentication—In Place and Planned

User identification in the form of a userid and password is required in order to gain access to any Sun workstation, SGI workstation, LAN server, and SwRI IBM mainframe or SwRI VAX computer. Formal written procedures exist for issuing these userids and passwords on some of these systems and informal procedures exist for the rest. Those that require formal procedures require that the user fill out a request form giving pertinent information and then the form must be signed by an approving Project Manager and CNWRA management. The system administrator of the LAN servers within the CNWRA will provide userid and passwords to users upon approval of that request by the Element Manager and/or concurrence by the IMS Director. More secure network authentication is planned for LAN access from outside of the firewall for those users wishing to gain access to the CNWRA LAN. Challenge-response cards will be issued to those users who meet prior approval by CNWRA management and NRC. The network will challenge the user to enter a encrypted password that is generated by the challenge-response card that they will be holding.

(ii) Authorization/Access Controls—In Place and Planned

There are inherent access control features in the various operating systems that make up the CNWRA LAN. In the UNIX operating system, there are userid and group ids that distinguish users, and directory and file permissions can be set to allow/disallow access accordingly. Other CNWRA and SwRI computers that are non-UNIX also have some file permission capabilities that are used to perform the same authorization/access control. The CNWRA plans to implement a firewall that uses a packet filter gateway mechanism and a router with an access control list. The filter table and access control list will be set up to allow/disallow access to and from the CNWRA LAN. This will provide additional access control capabilities.

(iii) Integrity Controls—In Place and Planned

The integrity controls that are in place are found in file transfer utilities that allow for verification of data once the data has reached its destination. Any nonvalidated data results in a checksum error.

(iv) Audit Trail Mechanisms—In Place and Planned

The current audit trail mechanisms are those found in the operating systems. System logs in some form are found on most of the CNWRA LAN servers. Also, logs exist that track the user login times and access times. The firewall packet filter gateway will provide logging capabilities when it is implemented. In addition, alerting capabilities will be used

18/
19

to signal pagers that a condition has been raised. Logs will show users that are authorized and not authorized to access the CNWRA LAN externally from the network. This will allow CNWRA to take appropriate action as soon as possible following an attempt at unauthorized access.

(v) **Confidentiality Controls—Planned**

Currently there is no encryption method used for transmission of data that is considered sensitive and predecisional in nature. Planned for encryption will be the use of challenge-response cards that pass network identification information encrypted over the network. Also planned is a centralized network backup system that will provide for the encryption of backed up data.

3.6.6 Controls Over the Security of Applications—In Place and Planned

Users of applications on the CNWRA LAN are given instructions for utilizing those applications in a manner that will not put the CNWRA LAN at risk. These instructions may direct the user to the CNWRA Computer Resource Guide that details instruction of the use of major applications. Other instructions may be provided in written form by the System Administrator. This will be an ongoing process as new applications are implemented on the CNWRA LAN.

19/19

4 REFERENCES

- Center for Nuclear Waste Regulatory Analyses. 1994a. *Evaluation of Potential Conflict of Interest, Administrative Procedure (AP-001) Revision 2, Change 2*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- Center for Nuclear Waste Regulatory Analyses. 1994b. *Quality Indoctrination and Training, Quality Assurance Procedure (QAP-005) Revision 0, Change 1*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- Center for Nuclear Waste Regulatory Analyses. 1994c. *Computer Network Access and Usage, Administrative Procedure (AP-014) Revision 0*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- Center for Nuclear Waste Regulatory Analyses. 1990. *Employment Procedures for Professional Staff, Quality Assurance Procedure (QAP-007) Revision 2, Change 2*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- DeWispelare, A.R., P.C. Mackin, J.H. Cooper, and R.L. Marshall. 1994. *User's Guide for Regulatory Program Database (RPD) Version 2.0 Including Open Item Tracking System (OITS)*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- Marshall, R.L, and A.L. Johnson. 1994. *CNWRA Network Security Proposal*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- Nuclear Regulatory Commission. 1992. *Instructions for Preparing Security Plans for Local Area Networks in Compliance with OMB. Bulletin No. 90-08. NUREG/BR-0166*. Washington, DC: Nuclear Regulatory Commission.
- Nuclear Regulatory Commission. 1994a. *Rules of Practice for Domestic Licensing Proceedings and Issuance of Orders*. Title 10, Energy, Part 2 (10 CFR Part 2). Washington, DC: U.S. Government Printing Office.
- Nuclear Regulatory Commission. 1994b. *Public Records*. Title 10, Energy, Part 9 (10 CFR Part 9). Washington, DC: U.S. Government Printing Office.
- Office of Management and Budget. 1990. *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*. OMB Bulletin No. 90-08. Washington, DC: Office of the Management and Budget.
- The Privacy Act*. 1974. 5 U.S.C. Section 552a. Washington, DC: U.S. Government Printing Office.
- Computer Crimes Act*. 1994. Public Law 103-322. Washington, DC: U.S. Government Printing Office.

**REGULATORY PROGRAM DATABASE (RPD)/
TECHNICAL REFERENCE DOCUMENT DATABASE
SYSTEM (TDOCS)
SECURITY PLAN**

Prepared for

**Nuclear Regulatory Commission
Contract NRC-02-93-005**

Prepared by

**Alfred L. Johnson
Robert L. Marshall
Rawley D. Johnson**

**Center for Nuclear Waste Regulatory Analyses
San Antonio, Texas**

January 1995

2/16

CONTENTS

Section	Page
FIGURES	iii
ACKNOWLEDGMENTS	iv
1 SYSTEM IDENTIFICATION	1-1
1.1 RESPONSIBLE ORGANIZATION	1-1
1.2 SYSTEM NAME/TITLE	1-1
1.3 SYSTEM CATEGORY	1-1
1.4 SYSTEM OPERATIONAL STATUS	1-1
1.5 GENERAL DESCRIPTION/PURPOSE	1-1
1.6 SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS	1-2
1.7 INFORMATION CONTACT(S)	1-2
2 SENSITIVITY OF INFORMATION HANDLED	2-1
2.1 APPLICABLE LAWS OR REGULATIONS AFFECTING THE SYSTEM	2-1
2.2 GENERAL DESCRIPTION OF INFORMATION SENSITIVITY	2-1
3 SYSTEM SECURITY MEASURES	3-1
3.1 RISK ASSESSMENT AND MANAGEMENT	3-1
3.2 APPLICABLE GUIDANCE	3-1
3.3 SECURITY CONTROL MEASURES	3-1
3.4 SECURITY CONTROL MEASURES STATUS	3-1
3.5 SECURITY CONTROL MEASURES FOR MAJOR APPLICATIONS	3-2
3.5.1 Management Controls—In Place and Planned	3-2
3.5.2 Development/Implementation Controls—In Place	3-2
3.5.3 Operational Controls—In Place	3-3
3.5.4 Security Awareness and Training—In Place	3-4
3.5.5 Technical Controls—In Place	3-4
3.5.6 Complementary Controls Provided by Support Systems—In Place	3-5
4 REFERENCES	4-1

FIGURES

Figure		Page
1-1	Current Center for Nuclear Waste Regulatory Analyses (CNWRA) San Antonio and Washington Technical Support Office (WTSO) network topology	1-4
1-2	Planned Center for Nuclear Waste Regulatory Analyses (CNWRA) San Antonio and Washington Technical Support Office (WTSO) network topology	1-5

4/16

ACKNOWLEDGMENTS

This report was prepared to document work performed by the Center for Nuclear Waste Regulatory Analyses (CNWRA) for the Nuclear Regulatory Commission (NRC) under Contract No. NRC-02-93-005. The activities reported here were performed on behalf of the NRC Office of Nuclear Material Safety and Safeguards (NMSS), Division of Waste Management (DWM). The report is an independent product of the CNWRA and does not necessarily reflect the views or regulatory position of the NRC.

The following trademarks are used in this report:

- OS/2 is a trademark of the International Business Machine (IBM) Corporation
- Macintosh is a trademark of Apple Corporation
- UNIX is a registered trademark of Unix System Laboratories, Inc.
- SPARCstation is a trademark of SPARC International, Inc.
- Wellfleet and Synoptics are trademarks of Bay Networks
- SGI is a trademark of Silicon Graphics, Inc.
- Ethernet is a trademark of Xerox Corporation
- VAX is a trademark of Digital Equipment Corporation

5/16

1 SYSTEM IDENTIFICATION

1.1 RESPONSIBLE ORGANIZATION

Center for Nuclear Waste Regulatory Analyses (CNWRA)

1.2 SYSTEM NAME/TITLE

Regulatory Program Database (RPD)/Technical Reference Document Database System (TDOCS)

1.3 SYSTEM CATEGORY

Major Application

1.4 SYSTEM OPERATIONAL STATUS

Operational

1.5 GENERAL DESCRIPTION/PURPOSE

The purpose of the RPD/TDOCS application is to support regulatory, technical, and institutional analyses in accordance with the Nuclear Waste Policy Act (NWPA), as amended. Under the NWPA, the Division of Waste Management (DWM) of the Nuclear Regulatory Commission (NRC) will regulate the U.S. Department of Energy (DOE) in its design, construction, operation, and closure of a high-level nuclear waste repository. The RPD/TDOCS, as implemented at CNWRA, consists of a single application which resides on the CNWRA Local Area Network (LAN) in San Antonio, Texas. Data stored in RPD/TDOCS is sensitive and not intended for disclosure, and the application is therefore declared sensitive.

The CNWRA LAN consists of approximately 7 UNIX Servers on an Ethernet LAN with approximately 80 OS/2 personal computers, 25 Sun workstations, and 10 Macintosh systems. The CNWRA organization is part of Southwest Research Institute (SwRI) and is connected to the SwRI LAN via a router. The CNWRA staff in San Antonio, Texas, are connected via a Wide Area Network (WAN) consisting of routers and a fractional T1 leased line to the NRC at Two White Flint North in Rockville, Maryland, and the CNWRA Washington Technical Support Office (WTSO) in Arlington, Virginia. Principal applications include both technical and information systems for Office Automation and Scientific and Engineering Computing, respectively. The LAN supports the sensitive application RPD/TDOCS.

The RPD/TDOCS application is an automated database and full-text management system for use by the NRC staff in managing regulatory program records, technical documents, correspondence, and other non-textual materials related to the prelicensing and licensing phases of the high-level radioactive waste (HLW) regulatory program. RPD/TDOCS is a client-server application using a Sun Sparcstation server, Sun, Macintosh and OS/2 clients, and the Network File System and Remote Procedure Call protocols of the Transmission Control Protocol/Internet Protocol suite for communications.

6/16

The CNWRA LAN became operational in October 1993. Following discussions of security requirements with the NRC during March–September 1994 and approval of the CNWRA Network Security Proposal (Marshall and Johnson, 1994) by Information Resource Management on November 18, 1994, a major modification to the LAN was begun to implement the firewall. It is projected that this modification will be completed in April 1995. Any references to the current topology reflect the LAN configuration as of the date of this security plan. Any references to the planned topology will reflect the LAN configuration at the completion of the approved firewall implementation in April 1995. This security plan was formatted to meet the guidelines given in NUREG/BR-0166 (Nuclear Regulatory Commission, 1992).

1.6 SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

The current CNWRA LAN topology is shown in Figure 1-1. The San Antonio CNWRA office is located in three separate buildings. Buildings 51 and 57 are served with a single ethernet segment, Building 189 is served by two Synoptics 3000 series concentrators. These two locations are connected together by one of the SwRI Cisco routers. The Wellfleet router connecting the San Antonio network to the NRC and to the CNWRA WTSO in Crystal City, Virginia is located on the first floor in Building 189.

The planned network topology is shown in Figure 1-2 and includes a CNWRA Firewall system equivalent to the NRC Firewall system. A new ethernet segment, the perimeter net, connects to the SwRI Cisco router through a new Cisco router (external router) which provides the first line of defense from the Internet. This perimeter net has its own distinct network number (subnet). A packet filter gateway connects the perimeter net to the internal CNWRA network. A second Cisco router (internal router) has been added to the internal network to route between the three buildings. A bastion host is located on the perimeter net to provide proxy services for Simple Mail Transfer Protocol, Domain Name Service, and Network News Transfer Protocol as well as to perform monitoring tasks for the perimeter net.

The RPD/TDOCS application depends upon the security features implemented as part of the CNWRA LAN for general access protection from the Internet. A separate security plan for the CNWRA is submitted as part of this milestone. In addition, the RPD/TDOCS application provides additional access control features, as well as configuration control and data validation capabilities in the server portion of the application.

1.7 INFORMATION CONTACT(S)

Rawley D. Johnson (CNWRA)
Director—IMS
(210) 522-5153

Robert L. Marshall (CNWRA)
Database Administrator—IMS
(210) 522-5248

Alfred L. Johnson (CNWRA)
Network Administrator—IMS
(210) 522-5238

7/16

Marvin Marshall [SwRI Computer and Telecommunications Center (CTC)]
Director—CTC
(210) 522-2298

George Stevenson (SwRI Security)
Manager—Security
(210) 522-5642

14

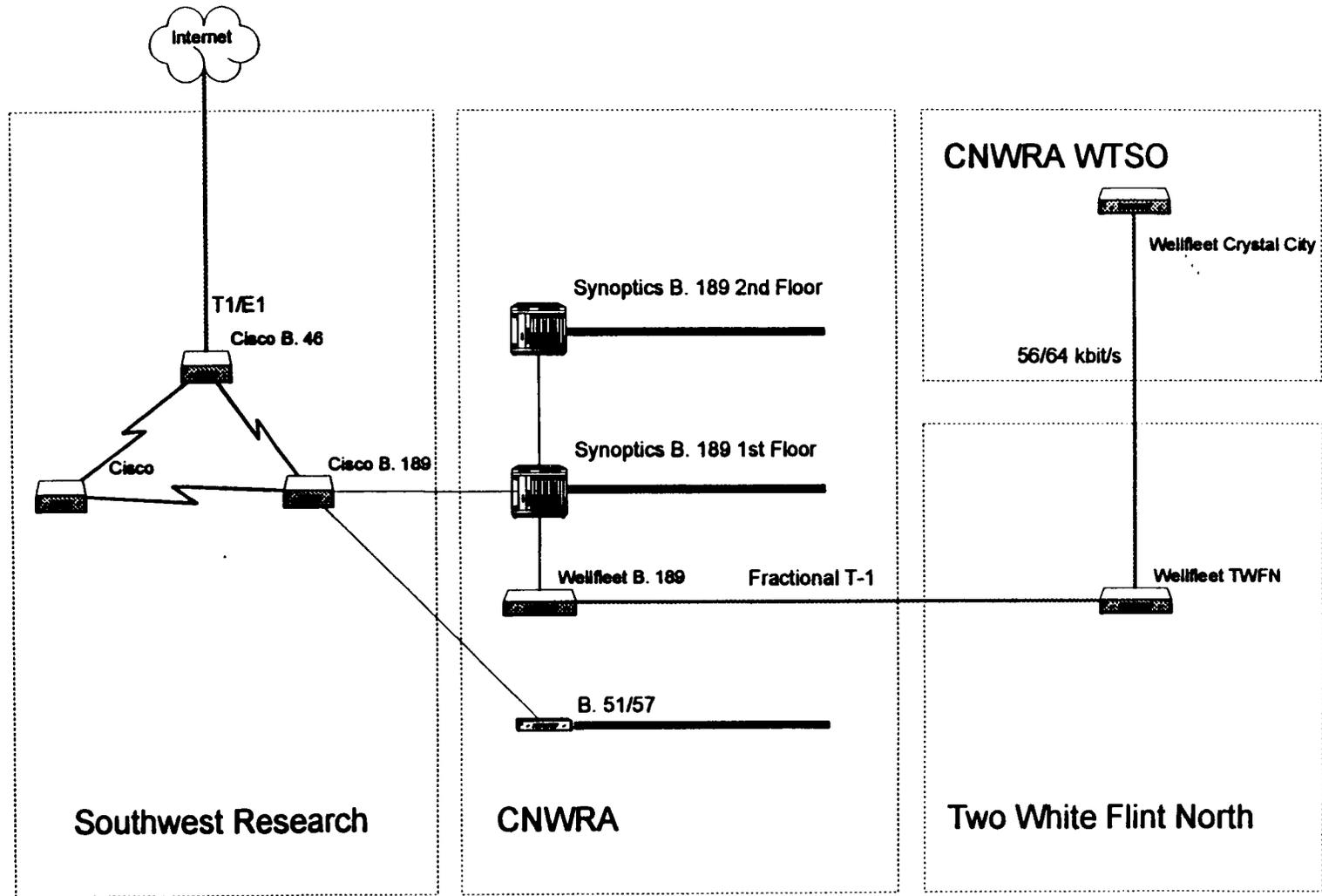


Figure 1-1. Current Center for Nuclear Waste Regulatory Analyses (CNWRA) San Antonio and Washington Technical Support Office (WTSO) network topology

2/1/8

1-5

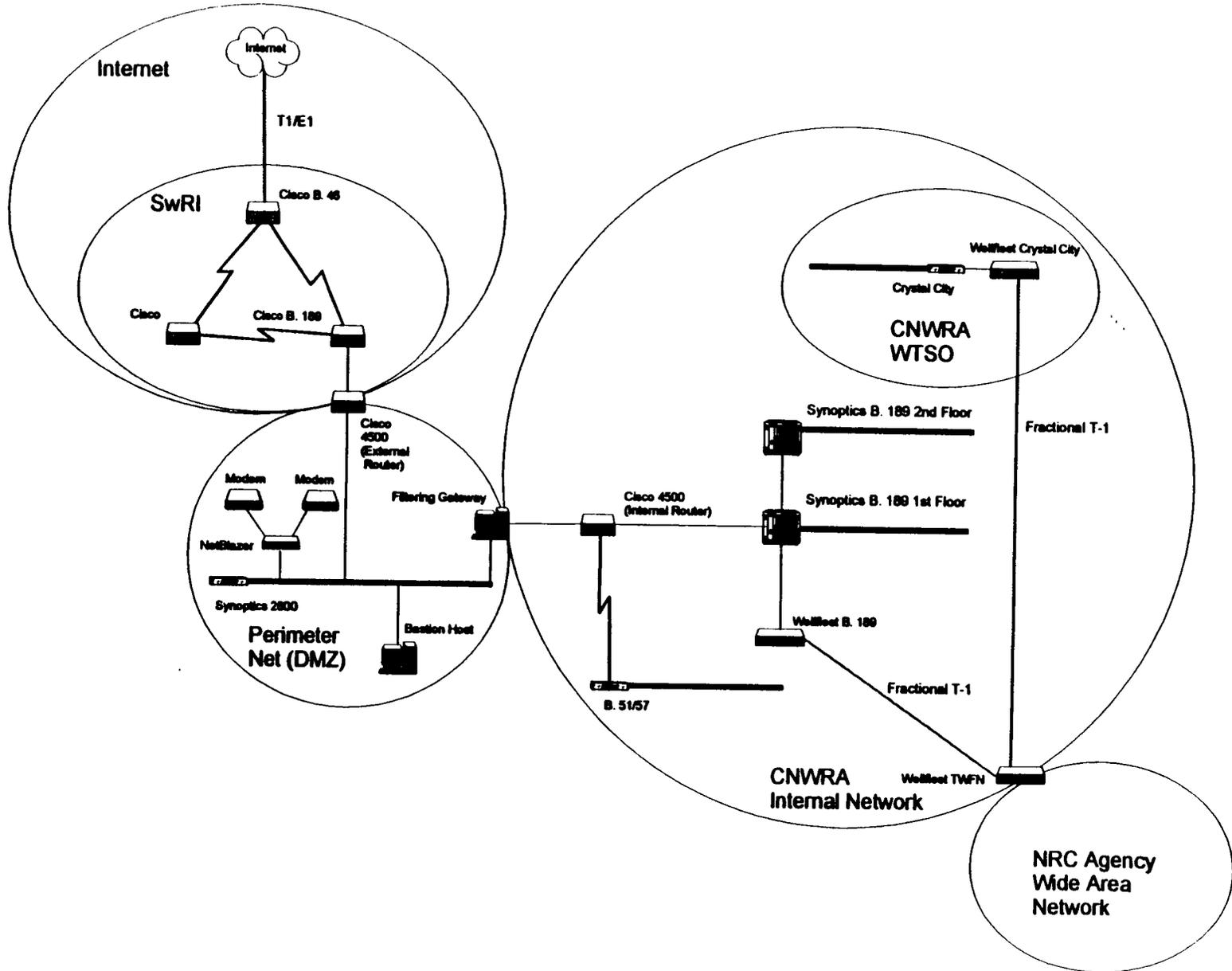


Figure 1-2. Planned Center for Nuclear Waste Regulatory Analyses (CNWRA) San Antonio and Washington Technical Support Office (WTSO) network topology

9/16

2 SENSITIVITY OF INFORMATION HANDLED

2.1 APPLICABLE LAWS OR REGULATIONS AFFECTING THE SYSTEM

Information maintained in the RPD/TDOCS application is covered by the Privacy Act of 1974 (5 U.S.C. Section 552a), 10 CFR Part 2 (Nuclear Regulatory Commission, 1994), and 10 CFR Part 9 (Nuclear Regulatory Commission, 1994) . An attempt to access the information stored in RPD/TDOCS in an unauthorized manner or damage the data in transit may be covered by the Computer Crimes Act of 1994 (Public Law 103-322).

2.2 GENERAL DESCRIPTION OF INFORMATION SENSITIVITY

(i) **Confidentiality-High**

RPD/TDOCS stores predecisional information used by DWM in implementing its responsibilities under the NWPA. This information is used to determine how the NRC might evaluate the DOE license for an HLW repository.

(ii) **Integrity-Medium**

The purpose of the RPD/TDOCS application is to search and retrieve data in support of regulatory analyses and prelicense and license review. Users of the application must be confident that the material is accurate. However, alteration of the contents would be more difficult because of its format (reports and documents) in contrast to scientific or engineering data.

(iii) **Availability-Medium**

The data stored in the RPD component is created via a manual off-line authoring process. The data stored in the TDOCS component consists of technical documents, electronically loaded or scanned, that can be found in books, journals, and paper correspondence logs. Lack of availability of the RPD/TDOCS data would not stop day-to-day operations but would increase costs to obtain the data from other sources.

11/16

3 SYSTEM SECURITY MEASURES

3.1 RISK ASSESSMENT AND MANAGEMENT

While risk analysis tools have not been used to perform a formal risk analysis of the RPD/TDOCS system, CNWRA staff members have performed an informal analysis of the RPD/TDOCS system and have identified potential risks. The following items are potential risks:

- There is a risk that the RPD/TDOCS system is exposed to compromise by creative UNIX and personal computer hackers with the competence to build viruses or dictionary-based password crackers.
- There is also a security risk from known operating system software deficiencies.
- There is a security risk in implicitly allowing external computers on the CNWRA LAN to have uncontrolled access to the RPD/TDOCS system.
- The CNWRA uses Internet services that provide for the transfer of data that will contain sensitive computer identification information (i.e., passwords) that is essential to maintenance of security of the RPD/TDOCS system. The use of an unsecured network application is a current risk.
- The procedures for assignment and maintenance of passwords on the RPD/TDOCS system is at risk if hackers can utilize "password cracking" tools to get access to those passwords.

3.2 APPLICABLE GUIDANCE

The following guidelines were used in the preparation of this security plan:

- OMB Bulletin No. 90-08: Guidance for Preparation of Security Plan for Federal Computer Systems that Contain Sensitive Information (Office of Management and Budget, 1990).
- NUREG/BR-0166: Instructions for Preparing Security Plans for LAN in Compliance with OMB Bulletin No. 90-08 (Nuclear Regulatory Commission, 1992).

3.3 SECURITY CONTROL MEASURES

Security control measures included in this plan have been addressed from the perspective of management and CNWRA staff directly responsible for the administration of the security for the LAN.

3.4 SECURITY CONTROL MEASURES STATUS

Specific management, operational, and technical measures that are either in place, planned, or in place and planned, are described in Section 3.5 of this plan.

3.5 SECURITY CONTROL MEASURES FOR MAJOR APPLICATIONS

3.5.1 Management Controls—In Place

(i) **Assignment of Security Responsibility—In Place**

The duties of system security officer have been assigned to the following individual:

Robert Marshall (CNWRA)
Database Administrator
(210) 522-5248

(ii) **Personnel Screening—In Place**

Personnel wanting to access the RPD/TDOCS application must first get authorization from the Element Manager of Waste Systems Engineering & Integration, Aaron DeWispelare, (210) 522-6072. Potential users are given access on the basis of their job function.

3.5.2 Development/Implementation Controls—In Place and Planned

(i) **Security Specifications—In Place and Planned**

Prior to development of the application, the requirements for user classes and authorization, password management, database security, file permissions, and user authorization were designed and documented. Additional security provisions for network access and physical access will be developed and implemented following the implementation of the LAN security system that supports the application.

(ii) **Design Review and Testing—In Place and Planned**

Following each phase of development of the application, a system test was performed that documented the extent to which the system met its design goals. Any deviations were corrected before starting the next phase of development. Additional system tests will be performed following each modification step.

(iii) **Certification—Planned**

The application will be certified in CNWRA Milestone 20-5702-157-540 in May 1995.

3.5.3 Operational Controls—In Place

(i) Physical and Environmental Protection—In Place

SwRI entrance is attended by security guards that check all unauthorized vehicles. Each building has locks to secure it and is locked by the guards before and after hours. Guards make periodic checks of each building. At CNWRA, each office has a lock on the door and the employee is provided with a key. Computer labs that have more than one computer also have locks on the door. The whole building has smoke alarms and fire extinguishers are installed in the event of a fire. Each computer is provided with a surge protector and every Sun workstation and major server also has an uninterruptable power supply in the event of loss of power.

(ii) Productions, Input/Output (I/O) Controls—In Place

Archival media are handled by the System Administrator. The media are labeled appropriately and stored in various locations depending upon frequency of their use. Short-term archives of the database are stored in the Database Administrator's office, and longer term archives may reside in the secure, fire-proof vault, locked in a room assigned to Quality Assurance.

(iii) Emergency, Backup, and Contingency Planning—In Place and Planned

The RPD/TDOCS system is backed up daily. Incremental and full backups are performed in the event of an emergency or disaster. These tapes are sent offsite once a month for storage. Only one copy of these tapes currently exists offsite. In the event of computer hardware failure, these tapes could be restored to another leased computer. CNWRA plans to acquire and implement a centralized network backup solution for the various computers, including the RPD/TDOCS system. This backup solution would perform centralized backups in the off hours over the network for all the CNWRA computers. This solution will also provide the capability to make a copy of the disaster recovery tapes that are being sent offsite, so that a copy could be retained in the CNWRA fire-proof vault as additional insurance.

(iv) Audit and Variance Detection—In Place

Audit and Variance Detection of the RPD/TDOCS database system is achieved by queuing all transactions to the ORACLE database and running a batch job in the evening to update the database. A record of the transactions is kept and can be rolled back in the event of corruption of the database. Backups are performed daily and the database can be recreated. In addition, ORACLE has a monitor that allows the Database Administrator to monitor activity and user's connection to the RPD/TDOCS database.

(v) Application Software Maintenance Controls—In Place

The RPD/TDOCS database system is under software configuration control (Center for Nuclear Waste Regulatory Analyses, 1994a). Modifications to the source code are tracked

14/116

through a product that is a part of a suite of tools used for software development. SPARCworks/TeamWare (SunPro, 1992) produced by Sun Microsystems, Inc., allows a team of programmers to work in parallel to develop software. The software tracks versions of the application, allows for merging of changes among different programmers, and provides for documentation of different revision levels. This product is used to ensure that the latest release of the application utilizes the most recent, up-to-date source code. SPARCworks/TeamWare also allows for generating any previous versions of the RPD/TDOCS application.

(vi) **Documentation—In Place**

Detailed descriptions of hardware and software components of the RPD/TDOCS database system are found in the RPD/TDOCS User Guide (DeWispelare et.al., 1994). The User Guide also details the RPD/TDOCS configuration in relation to the overall CNWRA LAN and provides detailed instructions on usage of the system. Instructions are given according to the level of authority assigned to the user's password.

3.5.4 Security Awareness and Training—In Place

No formal security awareness class for the RPD/TDOCS application has been organized at this time. However, as part of the RPD/TDOCS user training, security issues including user classes, password selection and management, and proper usage of RPD/TDOCS data are addressed. In addition, an administrative procedure (Center for Nuclear Waste Regulatory Analyses, 1994b) is in place to advise CNWRA personnel on proper use of computer systems and networks, a prerequisite to use of the RPD/TDOCS application. A seminar has been held to inform users of the security measures to be implemented as part of the CNWRA LAN firewall system and the RPD/TDOCS application.

3.5.5 Technical Controls—In Place

(i) **User Identification and Authentication—In Place**

User identification and authentication are in place by password control. Every authorized user of the RPD/TDOCS database system is given a userid and password. A level of usage is assigned to that userid and, as the level increases, more options are made available to that user in the form of menu items on the menu bar. Some examples are that the database may provide read-only versus read-write access, the capability to print reports, or perform full-text retrieval on certain databases.

(ii) **Authorization/Access Controls—In Place**

The RPD/TDOCS application does not allow for the user on the client side to get access to the operating system of the RPD/TDOCS server. On the client side, the RPD/TDOCS application relies on the underlying operating system to provide the authorization and access controls. If the clients use Sun workstations, a userid and password on that client workstation for the user provides control.

15/16

(iii) **Data Integrity/Validation Controls—In place**

The RPD/TDOCS database system relies on the underlying operating system to provide the data integrity. The userids, passwords, file permissions, and common UNIX data security are used to provide this control.

(iv) **Audit Trails and Journaling—In Place**

A chronological record of changes to the RPD/TDOCS database system is kept and changes to the database are archived. These logs have been traced to resolve problems with updates to the database in the initial stages of development.

3.5.6 Complementary Controls Provided by Support Systems—In Place

The database administrator and the network administrator responsible for the RPD/TDOCS application are also responsible for the security of the CNWRA LAN that the application depends upon and consult with NRC Information Resource Management personnel responsible for the security of the NRC LANs and Wide Area Network that access the application.

16/116

4 REFERENCES

- Center for Nuclear Waste Regulatory Analyses, 1994a. *Quality Assurance Manual, Revision 2, Change 6*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- Center for Nuclear Waste Regulatory Analyses, 1994b. *Computer Network Access and Usage. Administrative Procedure (AP-014) Revision 0*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- DeWispelare, A.R., P.C. Mackin, J.H. Cooper, and R.L. Marshall. 1994. *User's Guide for Regulatory Program Database (RPD) Version 2.0 Including Open Item Tracking System (OITS)*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- Marshall, R.L, and A.L. Johnson. 1994. *CNWRA Network Security Proposal*. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.
- Nuclear Regulatory Commission. 1992. *Instructions for Preparing Security Plans for Local Area Networks in Compliance with OMB. Bulletin No. 90-08*. NUREG/BR-0166. Washington, DC: Nuclear Regulatory Commission.
- Nuclear Regulatory Commission. 1994a. *Rules of Practice for Domestic Licensing Proceedings and Issuance of Orders*. Title 10, Energy, Part 2 (10 CFR Part 2). Washington, DC: U.S. Government Printing Office.
- Nuclear Regulatory Commission. 1994b. *Public Records*. Title 10, Energy, Part 9 (10 CFR Part 9). Washington, DC: U.S. Government Printing Office.
- Office of Management and Budget. 1990. *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*. OMB Bulletin No. 90-08. Washington, DC: Office of the Management and Budget.
- SunPro. 1992. *Code Managers User's Guide*. Sun Microsystems, Inc: Mountain View, CA.
- The Privacy Act*. 1974. 5 U.S.C. Section 552a. Washington, DC: U.S. Government Printing Office.
- Computer Crimes Act*. 1994. Public Law 103-322. Washington, DC: U.S. Government Printing Office.