CNWRA COMPUTER SECURITY PLAN

Prepared for

Nuclear Regulatory Commission
Contract NRC-02-88-005

Prepared by

Rawley D. Johnson

Center for Nuclear Waste Regulatory Analyses
San Antonio, Texas

February 1993

CONTENTS

CONTENTS (Cont'd)

FIGURES

ACKNOWLEDGMENTS

This report was prepared to document work performed by the Center for Nuclear Waste Regulatory Analyses (CNWRA) for the U.S. Nuclear Regulatory Commission (NRC) under Contract No. NRC-02-88-005. The activities reported here were performed on behalf of the NRC Division of High-Level Waste Management (DHLWM). The report is an independent product of the CNWRA and does not necessarily reflect the views or regulatory position of the NRC.

1 BASIC SYSTEM IDENTIFICATION

1.1 REPORTING ORGANIZATION

Center for Nuclear Waste Regulatory Analyses (CNWRA)

1.1.1 Organizational Subcomponent

Information Management Systems (IMS)

1.1.2 Operating Organization

Southwest Research Institute (SwRI) Computer & Telecommunications Center (CTC) and CNWRA IMS.

1.2 SYSTEM NAME

CNWRA Computer System

1.3 SYSTEM CATEGORY

Major Application

1.3.1 Level of Aggregation

Single Identifiable System

1.4 OPERATIONAL STATUS

Operational

1.5 GENERAL DESCRIPTION/PURPOSE

The purpose of the CNWRA Computer System is to support regulatory, technical, and institutional analyses in accordance with the Nuclear Waste Policy Act (NWPA), as amended. Under the NWPA, the High-Level Waste (HLW) Division of the U.S. 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 CNWRA Computer System is implemented and supported by the CNWRA in San Antonio, Texas.

1.6 SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

The current CNWRA Computer System configuration, as shown in Figure 1-1, consists of mainframe systems operated by the CTC at SwRI and a Local Area Network (LAN) with servers, personal computers and workstations operated by the CNWRA. The Wide-Area Network (WAN) is supported by the NRC and includes leased lines for telecommunications interfaces between the CNWRA's

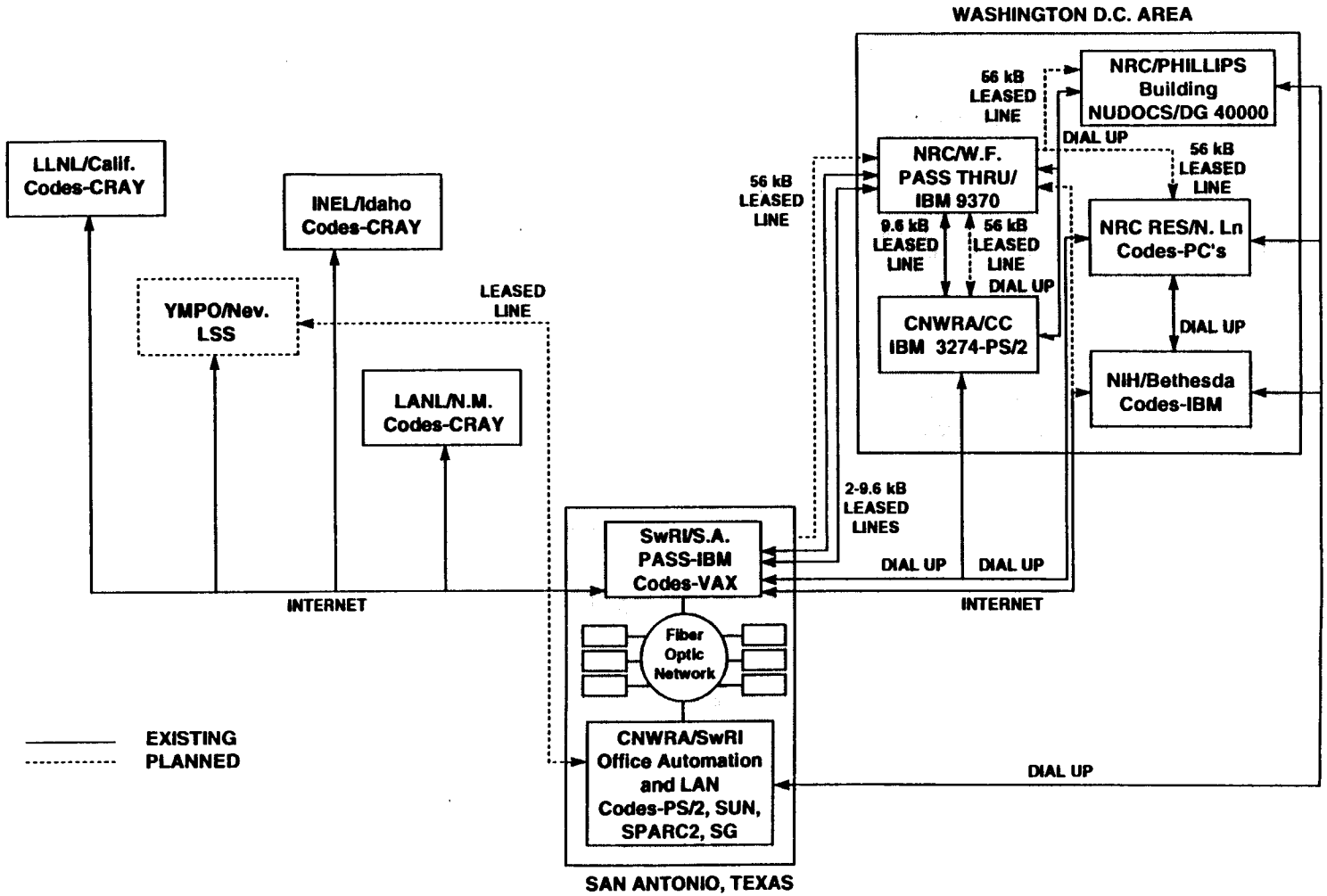

Figure 1-1. Current CNWRA Computer System configuration

San Antonio office and Washington Technical Support Office (WTSO) and the Division of High-Level Waste Management (DHLWM) in the One White Flint North (OWFN) building in Rockville, Maryland. The INTERNET is also used by the CNWRA for communications primarily in technical computing performed at Idaho National Engineering Laboratories (INEL) and Los Alamos National Laboratories (LANL).

The SwRI mainframe computer is an IBM 4381, operating under the XA Operating System, located in Building 46 in the CTC at SwRI in San Antonio, Texas. There are approximately 1250 users of this computer which is used for business and support services in addition to the CNWRA and NRC DHLWM users. Of these users, approximately 1200 are dedicated exclusively to the business office transaction processing and electronic timekeeping system; thus, cannot use any other application, such as the CNWRA's. The IBM 4381 and workstations for the CNWRA are connected on a fiber optic network at SwRI which also connects to a VAX 8700 in the CTC and various minicomputers in ten technical divisions. Two AT&T 9600 baud leased lines connect the IBM 4381 and VAX 8700 to a network of two IBM 9370 systems at the NRC OWFN Building, with a pass-through link via a leased line from White Flint to an IBM cluster controller in the CNWRA's WTSO in Arlington, Virginia.

The CNWRA is currently working with the NRC's Office of Information Resource Management (IRM) in their Agency Upgrade To Office Systems (AUTOS) and WAN programs to increase the speed of the leased telecommunications lines from 9.6 kbps to 56 kbps and install routers in each of the CNWRA offices interfaced to the NRC in OWFN as shown in Figure 1-2. It is expected that this upgrade will be operational in March 1993.

At the present time, there are approximately 61 workstations in the CNWRA's San Antonio Office with direct lines or LAN connections which provide access to the IBM 4381 and VAX 8700, as well as, and the Silicon Graphics IRIS and SUN Sparc2 ARC-INFO System located in Building 168. These user workstations are located on the third floors of Buildings 168 and 178 and in Building 57 at SwRI. Six additional workstations are located in the CNWRA's WTSO at Crystal Gateway One, Suite 1102, in Arlington, Virginia. Approximately 13 workstations can be used to access the IBM 4381 and VAX 8700 from the NRC DHLWM offices in White Flint.

All of the offices in San Antonio, in which these workstations are located, plus the computer room for the IBM 4381 and VAX 8700 in Building 46 in San Antonio, are controlled by means of combinations of guards, key-cards, and locks. All of the workstations and LAN-supported access require that a User Identification and Password be entered to logon and access the IBM 4381 and VAX 8700. In addition, there are certain restrictions on some User Identifications that limit them to read-only processes and also define the levels and types of data that may be read. Only four closely controlled User Identification have "write" privileges for the CNWRA controlled databases on the IBM 4381. To access any of the databases on the IBM 4381 or VAX 8700 in an approved manner, a person would have to have physical access to a system terminal, training to put the terminal into a user mode, and know the required Password. Password and access privileges for the CNWRA are administered by the Director of IMS for the CNWRA, the database administrator, and a systems manager.

SwRI is a member of the INTERNET. To gain access from the INTERNET to the IBM 4381 or VAX 8700 CNWRA controlled databases, a person would need to know that the databases are on the IBM 4381 or VAX 8700, obtain the INTERNET address of the IBM or VAX, and would need to know the user identification and password to access that data.

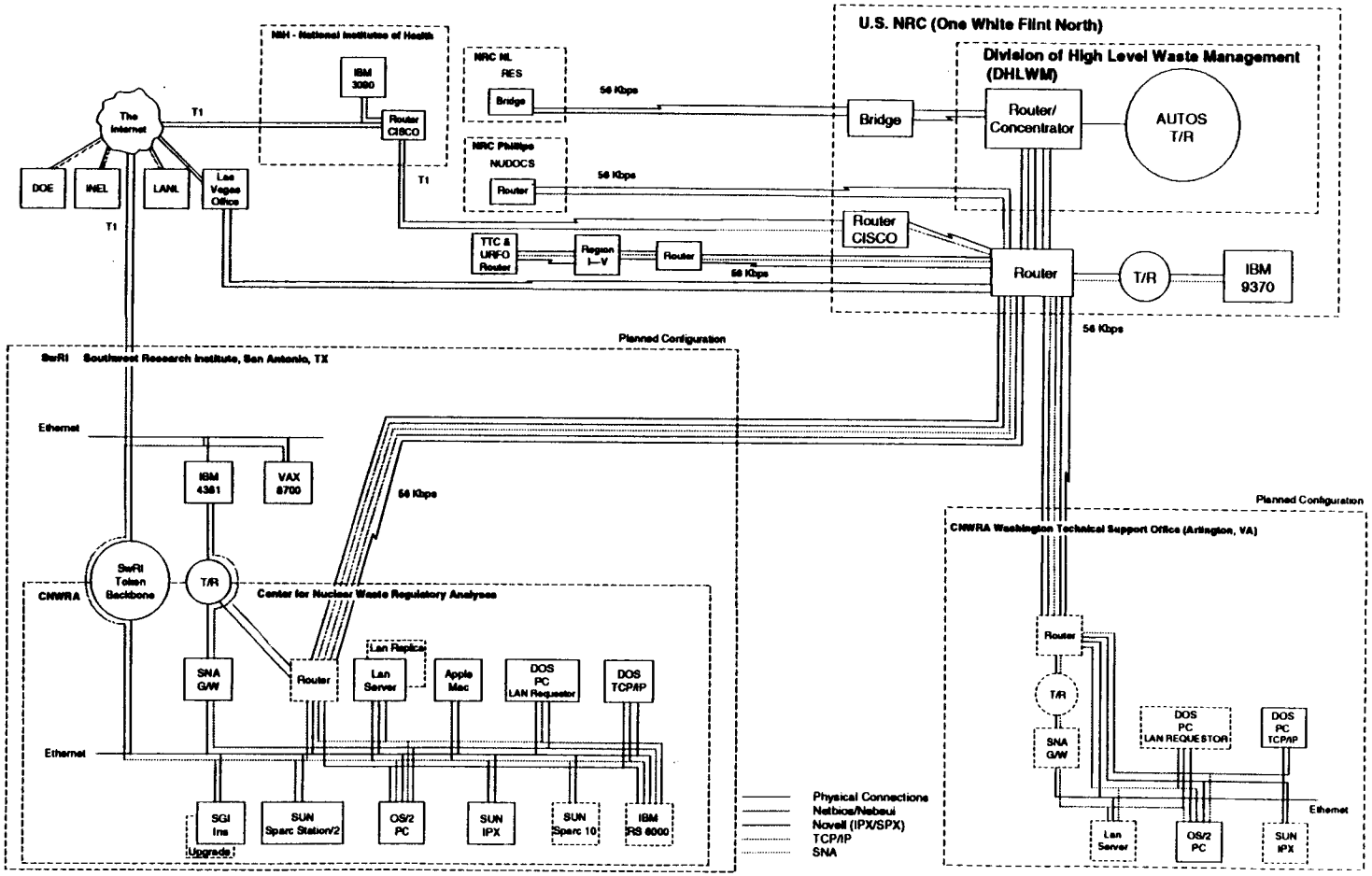

Figure 1-2. Planned CNWRA Computer System configuration

Security planning is underway for the interface of the CNWRA Computer System to AUTOS and the NRC WAN upgrade. Initially, the CNWRA staff will have no privileges to any AUTOS servers or requestors and this will prohibit an outsider on INTERNET coming into the CNWRA LAN and passing through as an impostor to the AUTOS.

1.7 INFORMATION CONTACTS

Rawley D. Johnson (CNWRA), 512/522-5153
Director - IMS

Don R. Saathoff (SwRI CTC), 512/522-2559
Director - CTC

George Stevenson (SwRI Security), 512-522-2111
Manager - Security; SwRI

2 SENSITIVITY OF SYSTEM OR DATA HANDLED

The general description of data or systems sensitivity for the CNWRA Computer System is provided in this section.

The CNWRA Computer System supports four major functions and associated data applications. A general description of the data and system sensitivity for each is provided below with Figure 2-1 displaying the functional relationships for each data application.

- Systematic Regulatory Analysis (SRA)

  The Program Architecture Support System (PASS)/Program Architecture Data Base (PADB) is used to capture results of SRA, support the efficient retrieval, review and status of information, and support and maintain a corporate memory of decisions and considerations pertaining to the licensing process. A regulatory text feature provides keyword search, retrieval and display of all applicable statues, regulations and other supporting information, as appropriate. PASS/PADB provides a logical structure and physical mechanism for storing results of the SRA being performed in support of the HLW Program. The PASS/PADB implementation is incorporating an "open item" tracking system for programmatic, technical, and administrative open items.

  The data in the PASS/PADB on the CNWRA Computer System that results from SRA is considered to be privileged data for use by the NRC and the CNWRA in support of the HLW program regulatory actions under the NWPA.

- Office Automation and Document Control

  The Office Automation function is vital to the exchange of information on the HLW Program. In addition, it is the infrastructure that provides the necessary tools for the daily communications among the CNWRA and NRC staffs. Specific functions include Electronic Mail, Word Processing, Correspondence Control, Technical Document Indexing, and Quality Assurance (QA) Document Indexing.

- Project Management

  The Project Management function supports the administration of operations planning, periodic cost reporting, commitment control, and project scheduling in the CNWRA.

- Scientific and Engineering Models and Codes

  The scientific and engineering models and codes are used in support of Performance Assessment and technical assistance for all the program elements and various research projects in the CNWRA.

  The CNWRA's technical assistance includes review of activities and development of guidance, procedures, and technical positions. In fulfilling this task, there is significant access of technical databases, analysis and display of spatial and temporal data, code

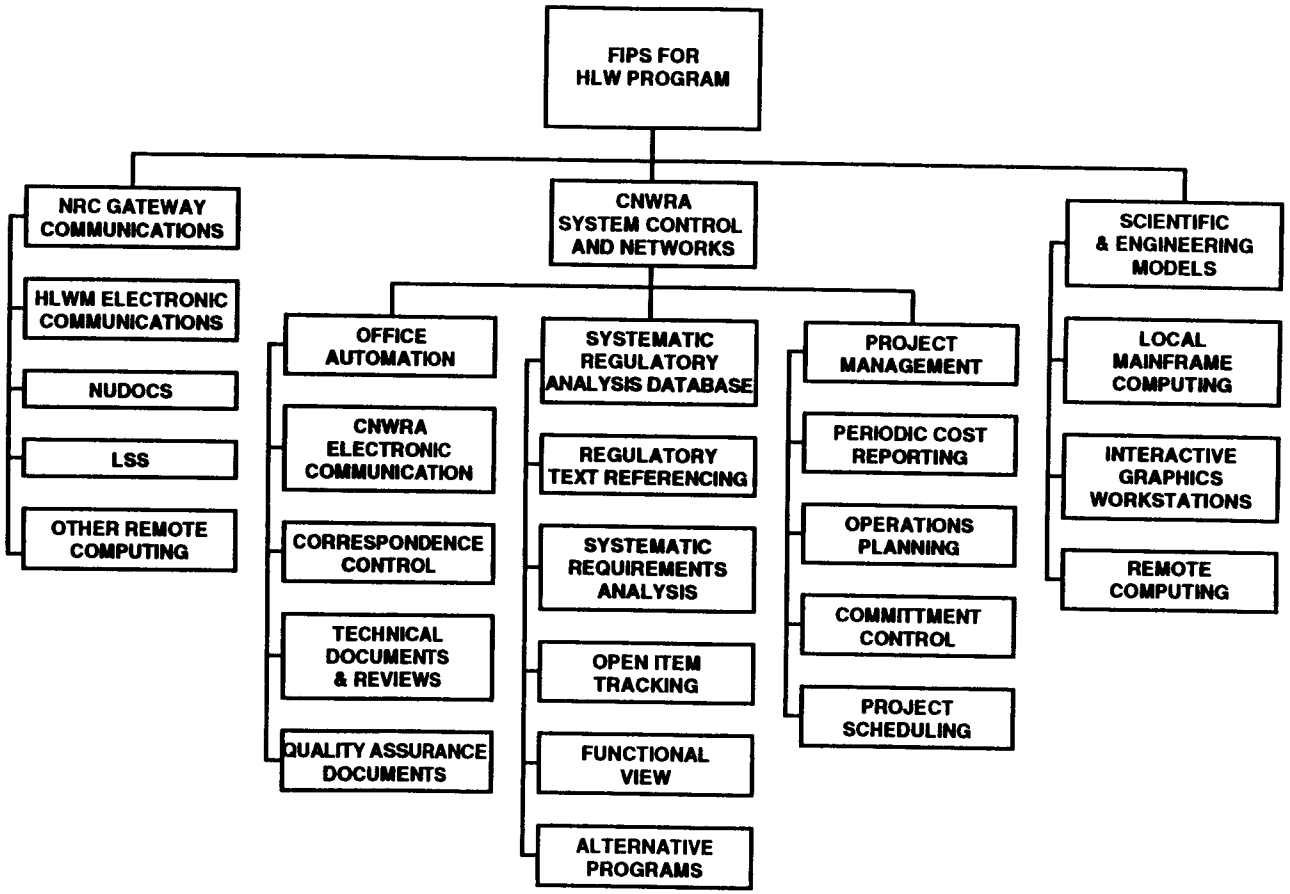

Figure 2-1. CNWRA Computer System functional relationships for HLW program

assessments, and literature searches and review, as well as checking DOE calculations and text. The CNWRA's Research Program is directed at reducing and/or resolving technical uncertainties in the HLW repository licensing program. Evaluations using models and codes for investigation of important technical areas, such as Unsaturated Mass Transport (geochemistry), Thermohydrology, Seismic Rock Mechanics, Integrated Waste Package Experiments, Stochastic Analysis of Flow and Transport, Geochemical Analogs and Modeling Sorption Mechanism, are underway.

2.1 APPLICABLE LAWS OR REGULATIONS AFFECTING THE SYSTEM

Information processed by the CNWRA Computer System is subject to the provision of the Freedom of Information Act (5 U.S.C. 552), Privacy Act (5 U.S.C. 552a), 10 CFR Part 2, "Rules of Practice for Domestic Licensing Proceedings," and 10 CFR Part 9, "Public Records."

2.2 GENERAL DESCRIPTION OF INFORMATION SENSITIVITY

System protection requirements for the four functions of the system are indicated in the following table.

Functions	Availability	Integrity	Confidentiality
Office Automation and Document Control	High	Medium	Low
SRA	High	High	Medium
Project Management	Medium	High	High
Scientific and Engineering Codes	Medium	High	Low

2.3 NEED FOR PROTECTIVE MEASURES, RELATED TO INFORMATION SENSITIVITY

The primary system protection requirements in Section 2.2 are for timely availability of the information and integrity of the data. Since much of the information will be made available in plans and reports from the NRC to the DOE as the license application process progresses, the confidentiality of the data is of secondary importance.

2.4 ESTIMATED RISK FOR SYSTEM PROTECTION

Risk Assessment: Informal Risk Analysis

Because of the early implementation phase of the CNWRA Computer System, the unavailability or lack of integrity of data will minimally impact the program at this time. However, the data volume will increase significantly between now and the time for the review of the license and all three items will be of more concern.

2.5 LEVEL OF PROTECTION REQUIREMENT (HIGH, MEDIUM, LOW)

The risk and protection requirements were determined to be medium by a review of system documentation and reports, interviews with NRC and CNWRA staff, the SwRI Security Officer, CTC Director, and CNWRA end-users.

2.6 OTHER INFORMATION

None.

3 SYSTEM SECURITY MEASURES

3.1 RISK ASSESSMENT MANAGEMENT

One of the major risks of the system is the loss of data, since much of the data is text and created and loaded day-by-day. Therefore, the lost time in data preparation and input and the unavailability of information are highest priority in risk assessment management.

3.2 APPLICABLE GUIDANCE (AGENCY POLICY, GUIDELINES)

- OMB Bulletin No. 90-08: Guidance for Preparation of Security Plans for Federal Computer Systems that contain Sensitive Information.
- The Computer Security Act of 1987 (P.L. 100-235).
- OMB Circular No. A-130, Appendix III, "Management of Federal Information Resources" (A-130).
- NRC Appendix 2301, Security of Automated Information Systems, July 25, 1985, Part 2, Paragraph A.1, Requirements for Unclassified Systems Processing Sensitive or Unidentified Data.

3.3 SECURITY CONTROL MEASURES

Controls included in this plan have been addressed from the perspective of management directly responsible for the system.

3.4 SECURITY CONTROL MEASURES STATUS

Every computer system, regardless of size or complexity of application, must employ safeguards to ensure the security of the data processed or stored within it. Computer security is an integration of elements from a variety of different fields. The current computer security measures in place and planned for the ongoing support of the CNWRA Computer System are provided in the following sections.

3.5 SECURITY CONTROL MEASURES FOR MAJOR APPLICATIONS

3.5.1 Management Controls

3.5.1.1 Assignment of Security Responsibility

The three individuals identified in Section 1.7 under Information Contacts have computer security responsibility at SwRI, CTC, and CNWRA for their respective areas of this major system and its functions.

3.5.1.2 Personnel Screening

Adequately trained CNWRA and NRC staff plus a number of the staff actively using the system have appropriate security clearances. Personnel qualification under the CNWRA's QA Program is also performed and documented.

3.5.2 Development/Implementation Controls

3.5.2.1 Security Specification

The CNWRA's QA Program addresses the personnel qualifications in regard to technical requirements, the CNWRA Management Plan addresses the administration matters, and a Configuration Management and Control Manual and Technical Operating Procedure, "Configuration Management of Scientific and Engineering Computer Codes" (TOP-018), address physical control and personnel security.

3.5.2.2 Design Review and Testing

Modifications to the currently operating CNWRA Computer System are developed and tested in phases. Reviews are performed at the conclusion of each phase with appropriate documentation and acceptance by the NRC.

3.5.2.3 Certification

An internal QA audit is performed annually of all CNWRA Computer Systems by the SwRI QA staff, with observers from the NRC DHLWM staff.

3.5.3 Operational Controls

3.5.3.1 Physical and Environmental Protection

Protection of the CNWRA and NRC staff work areas and workstations is accomplished by means of guard stations and/or key-card devices when entering the building. The computer room for the IBM 4381 and VAX 8700 are locked and/or operator controlled at all times. The workstations for all of the various users of the system at SwRI are in locked buildings when unattended by the staff on weekends and overnight. Each building has a guard or receptionist on duty during normal working hours and at break times during the day.

3.5.3.2 Production and Input/Output Controls

All archival material (tape) is handled by the system operator. The operator is trained to label such media appropriately as directed by CNWRA staff. Archival media are stored only in the operator room, the CNWRA Computer Room, and an off-site storage location. Media are to be released only to CNWRA IMS staff. Paper output is produced at the CNWRA buildings. All retained paper output is controlled by CNWRA administrative procedures. All waste paper output is recycled by a bonded third party.

3.5.3.3 Emergency, Backup and Contingency Planning

All data on the IBM 4381, VAX 8700 and CNWRA servers is backed up daily. The archival media (tape) are stored in a location removed from SwRI campus. The archives would be used to restore the systems, both programs and data, for CNWRA. The system would be restored to leased system or to commercial system. Due to the increasing commonality of hardware between the SwRI and the NRC, the majority of the system could be restored to the NRC system, given sufficient resources.

3.5.3.4 Audit and Variance Detection

Audit procedures exist to capture violations of established procedures. For example, invalid logon attempts to the IBM 4381 are noted in a log. System and database usage statistics and costs are captured. These are used to build execution profiles for system and application capacity planning and tuning.

3.5.3.5 Application Software Maintenance Controls

The CNWRA uses a configuration management and control procedure for all pertinent software development and maintenance. All changes made to the application software are logged in a database and a historical record is maintained of the changes. Appropriate review, approval, and testing is done commensurate with the level of the change.

3.5.3.6 Documentation

Controls in the form of requirements definitions for new application systems, specifications, program descriptions, users guides and implementing procedures for users are available. Adequate documentation is maintained by the developers to permit continuity in development and for the end user to maintain continuity in operation of the systems.

3.5.4 Security Awareness and Training Measures

All employees involved with the management, use, design, development, maintenance, or operation of the system are aware of their responsibilities and are trained on the job and attend weekly operations meetings.

3.5.5 Technical Controls

3.5.5.1 User Identification and Authenticity

Procedures exist for issuing User Identifications and Passwords for the system. A request form must be completed giving the user's name, company, project charge number, phone number and signed off by an approving Project Manager and division management. The desired User Identification is indicated on the form, the initial (first computer session) Password desired is also entered, and the form is submitted to the System Administrator for approval and setting up on the system. The passwords employed must be five to eight characters in length. On some of the workstations used for software development and LAN supported access, an additional Password is required before anyone could use the

workstation, LAN, or the system. In addition, specific procedures are used for designating who has read/write privileges authorized on the system.

3.5.5.2 Authorization/Access Controls

Use of the system is controlled by a user authorization list. There are multiple levels of authority implemented. General users may only view final, reviewed data. Analysts preparing data may view unreviewed data relevant to their development activities. Update, insert, and delete operations of databases are restricted to single maintenance user identification. These levels of access are under program control and administered by the Database Administrator.

3.5.5.3 Data Integrity/Validation Controls

Data integrity is maintained primarily by access controls. There is some limited validity checking of data entered into databases. There are extensive verification checks made of data and calculations in engineering codes.

3.5.5.4 Audit Trails and Journaling

Data in the relational database is controlled by the logging facilities of the database product. This provides for unit-of-work integrity. Unit-of-work integrity means that none of the changes to the database are finalized until all of the changes are complete (committed). If any change fails, the intermediate changes are removed (rolled back), and the database is restored to its previous state. Textual data is not protected by a transaction processor, but may be recovered to the previous day's level by means of the nightly backup media.

3.5.6 Complementary Controls Provided by Support Systems

All systems included in the CNWRA Computer System application are included in the information above. The network communication system between SwRI in San Antonio, CNWRA in San Antonio and Arlington, Virginia, and the NRC in White Flint is the responsibility of the NRC.

4 ADDITIONAL COMMENTS

At this stage in the development of the CNWRA Computer System, the security measures currently in place and implemented are appropriate and adequate. It is recommended that the array of CNWRA and SwRI security measures now in effect be maintained at current levels to ensure system environment integrity until the Licensing Support System (LSS) is brought on line. At the time the LSS is brought up and NRC makes a determination regarding the connection of the CNWRA Computer System to the LSS and/or its contribution of data to the LSS, additional LSS-equivalent security measures may become mandatory.

However, according to the Computer Security Act of 1987 and Office of Management and Budget (OMB) guidance, security plans are required to be reviewed and updated every five years, unless there is a major change to the system (e.g., new location, new or additional hardware, or new major software applications). Therefore, this version will be updated in FY94, since according to IRM policy, both the LAN/WAN upgrades and move to a new building in San Antonio dictate that this be done. This approach to the CNWRA Computer System environmental security is both cost-effective and is in parallel with NRC measures to provide security to database, hardware, and software systems.