United States Nuclear Regulatory Commission
Office of the Chief Information Officer
Information Technology Infrastructure Division

INFRASTRUCTURE SERVICES AND SUPPORT CONTRACT

CURRENT ITID INFRASTRUCTURE SERVICES

June 4, 2001

TABLE OF CONTENTS

1 CUSTOMER SUPPORT CENTER . . . 5
1.1 CSC Help Desk Operations . . . 5
1.1.1 CSC Service Request Preparation . . . 5
1.1.2 CSC Service Request - Problem Requests . . . 6
1.1.3 CSC Service Request - End-user Questions . . . 6
1.2 SWAT Requests . . . 7
1.3 Special Handling . . . 7
1.4 Knowledge Bases . . . 7
1.5 Web Enabled Services . . . 7
1.6 Reporting . . . 7

2 DESKTOP SERVICES . . . 8
2.1 Maintenance . . . 8
2.1.1 Hardware Maintenance . . . 8
2.1.2 Spare Parts . . . 9
2.1.3 Special Maintenance . . . 9
2.1.4 Software Maintenance . . . 9
2.1.5 Diagnostic Utilities . . . 9
2.1.6 Warranties . . . 9
2.1.7 Reporting . . . 10
2.2 Installation/Deployment . . . 10
2.2.1 CSC Service Requests . . . 10
2.2.2 Network Coordination . . . 10
2.2.3 Hardware Coordination . . . 10
2.2.4 Software Coordination . . . 11
2.3 ADAMS Support . . . 11
2.4 Non-Infrastructure Acquisitions . . . 12
2.5 Procurement . . . 12
2.5.1 Hardware/Software . . . 12
2.5.2 Spare Parts . . . 12

3 NETWORK SERVICES . . . 13
3.1 Network Operations Center (NOC) . . . 13
3.2 Current NOC Operations . . . 14
3.2.1 Network Management . . . 14
3.2.2 CSC Service Requests . . . 15
3.2.3 Failures . . . 15
3.2.4 Service Provisioning . . . 16
3.2.4.1 Remote Access System . . . 16
3.2.4.2 Resident Inspector Sites Frame Relay Connections . . . 16
3.2.4.3 WAN Connectivity . . . 16
3.2.5 On-call Operations . . . 16
3.3 Maintenance . . . 16
3.3.1 Hardware Maintenance . . . 16
3.3.2 Spare Parts . . . 17
3.3.3 Software Maintenance . . . 17
3.3.4 Special Maintenance . . . 17

3.3.5 Reporting 17
3.4 Installation/Deployment 18
3.4.1 New Systems 18
3.4.2 Relocations 18
3.5 Procurement 18
3.6 Regional LAN Administrator Support 18

4 INFRASTRUCTURE DEVELOPMENT AND IMPLEMENTATION SERVICES 22
4.1 Systems Engineering 22
4.1.1 IT Infrastructure Development 22
4.1.2 IT Infrastructure Integration 22
4.1.3 IT Infrastructure Implementation 22
4.2 IT Infrastructure Services 23
4.2.1 Workstation System Services 23
4.2.2 Local and Wide Area System Services 23
4.2.2.1 Infrastructure Services 23
4.2.2.2 Web Architecture Services 23
4.2.2.3 LAN/WAN Server Services 23
4.2.3 High Performance Computing Environment (HPCE) Services 23
4.2.4 Other IT Infrastructure Services 24
4.2.4.1 IT Infrastructure Security Services 24
4.2.4.2 Contingency Management 24
4.2.4.3 Procurement 24
4.3 Development, Integration, and Implementation Life-Cycle 25
4.3.1 Detailed Requirements Analysis 25
4.3.2 Design 25
4.3.3 New Technology Development 26
4.3.4 New Technology Acceptance Testing 26
4.3.5 Transition to Production Operational Support 26
4.3.6 Implementation 27
4.3.7 Position Descriptions 27

5 PROGRAM SERVICES 35
5.1 Quality Management 35
5.1.1 Program Management 35
5.1.2 Metrics and Performance Criteria 35
5.1.3 End-User Satisfaction Monitoring 35
5.1.4 Trend Analysis 35
5.1.7 Audits 36
5.2 Configuration Management 36
5.2.1 Program Management 36
5.2.2 Change Management 36
5.2.3 Hardware/Software Inventory 36
5.2.4 Configuration Management Data Base (CMDB) 37
5.2.5 Configuration Reporting 37
5.3 Contingency Management 37
5.3.1 Program Management 37
5.3.2 Backup 37
5.3.3 Disaster Recovery 37
5.4 Documentation Management 38

5.4.1 Program Management 38
5.4.2 Procedures 38
5.5 Security Management 38
5.5.1 Program Management 38
5.5.2 System 38
5.5.3 Network/Cyber 39
5.5.4 Physical 39
5.5.5 Audits 39
5.6 Independent Audit and Verification 40

6 RELATED NRC IT SERVICES 41
6.1 TELECOMMUNICATIONS SERVICES 41
6.2 DATA CENTER SERVICES 41
6.3 EMERGENCY OPERATIONS CENTER 42

1 CUSTOMER SUPPORT CENTER

The Customer Support Center (CSC) Help Desk provides single point of contact for primary immediate IT support and assistance to NRC end-users. The CSC is responsible for providing a single common telephone number for assisting the NRC HQ staff in the proper use and maintenance of the NRC IT infrastructure systems and applications used to accomplish the mission and program activities of the NRC. The CSC provides first-line problem diagnosis and resolution for desktops, networks, telephones, Agencywide applications, Agency-developed applications, minicomputers, mainframe computers, and timesharing services.

The CSC provides Tier 1 (telephone) support, which includes problem resolution, reporting, assigning, tracking, and escalation services for NRC end-user reported questions, problems, and requests for new or changed services related to IT Infrastructure systems and applications. The CSC responds by telephone to end-user requests for common operational problems and questions. The CSC is responsible for resolving operational problems using remote diagnostic and correction facilities whenever possible. If required, CSC Tier 1 support includes CSC assignment of the initial action to the appropriate support group, however CSC maintains responsibility for processing, prioritizing, escalating, and tracking CSC Service Requests to closure.

The Regions currently provide Help Desk services, installation, warranty and out-of-warranty maintenance to their Regional offices and their Resident Inspector sites.

1.1 CSC Help Desk Operations

The CSC Help Desk provides support for NRC Headquarters user questions and service requests, coordinates support activities with other support components, and confirms customer satisfaction with the service provided.

This group is responsible for assignment of the initial action to the appropriate group and follow-thru to closure of the CSC Service Request.

- Provide problem resolution, reporting, assigning, tracking, and escalation services for NRC end-user reported questions and problems related to desktop systems hardware and software, the NRC network, NRC Telecom services, Data Center, and timesharing services.
- Answer all telephone calls to the CSC
- Respond by telephone to requests from: Email, memos, voice-mail, NRC forms, the OCIO desktop support group, or the Network Operations Center in accordance with service level requirements.
- Resolve the customers request on the first phone call whenever possible

1.1.1 CSC Service Request Preparation

- The CSC utilizes the McAfee automated system to track and report on Service Requests.
- Create a CSC Service Request utilizing the CSC Service Request Tracking System for each end-user reported problem or question.

- Notify customers of the CSC Request Number assigned to a Service Request.
- Establish the problem severity level on each CSC Service Request.
- Change priority on open CSC Service Requests as needed.
- Maintain ownership of CSC Service Requests and monitor progress until problem resolution.
- Contact the end-user to provide CSC Service Request status updates and anticipated problem resolution.
- Confirm that problems are resolved to customer satisfaction.
- Close CSC Service Requests upon customer confirmation of resolution.

1.1.2 CSC Service Request - Problem Requests

- Create a CSC Service Request for every end-user reported problem.
- Resolve end-user problem over the telephone or remotely whenever possible.
- Provide knowledge base, troubleshooting and diagnostic support to identify and resolve end-user problems.
- Resolve problems related to desktop systems such as incorrect set-up, customization, incorrect use of the system, and user changes to standard configurations, etc.
- Resolve routine network-related items such as LAN printer problems, password resets, LAN disk space allocations, and workstation Network software.
- Analyze, diagnose, and resolve problems from a total NRC systems perspective.
- Respond to recurring problems.

1.1.3 CSC Service Request - End-user Questions

- Create a CSC Service Request for every end-user question.
- Respond to end-use questions related to:
    - The procurement of IT resources.
    - The utilization of supported hardware and software.
    - The utilization of supported commercial off-the-shelf (COTS) software.
    - The utilization of all Agency wide systems.
    - The utilization of NRC developed applications.
    - Requests for general information.

1.2 SWAT Requests

- Coordinate SWAT (scheduled work activities) requests among the OCIO support groups to assure resolution of problems that cannot be resolved over the telephone, by on-site support, or by consulting services.

1.3 Special Handling

- Respond to requests for special handling, escalation, or higher priority on specifically identified requests.
- Escalate requests to a higher level of support in accordance with NRC policies, procedures and service level requirements.

1.4 Knowledge Bases

- Maintain an automated knowledge base of information to facilitate user support and end-user self-help.
- Maintain the knowledge base and keep it updated with current information as problem resolutions become known.
- Utilize the knowledge base whenever applicable.

1.5 Web Enabled Services

- Maintain a web-accessible database to allow users to monitor CSC Service Request status.
- Maintain on a monthly basis, a web-accessible database of end-user frequently asked questions (FAQ).

1.6 Reporting

- Prepare briefings and attend the daily CSC operational status meeting as requested.
- Prepare briefings and attend the weekly operational status meeting as requested.
- Prepare the summary report for the monthly CSC performance report.

2 DESKTOP SERVICES

Desktop Services provide all NRC personnel with a standard desktop workstation that is an Intel-based processor using the Microsoft NT Workstation operating system. Desktop Services also provides installation and all Tier 2 (on-site) maintenance and upgrade services to HQ Offices. Desktop installation and maintenance and Tier 2 support in the Regions is supplied by the Regions.

Headquarters Desktop Services is broken into three areas:

PC Refresh. Replacement of the desktop (or equivalent) business application microcomputer inventory for the entire Agency.

During 1997-1999, most of NRC PC's were upgraded for Y2K compliance. The current NRC budget allocates funds for a 15% refresh rate. Funds available at the end of each fiscal year are also sometimes allocated to equipment refresh if an upgrade requirement is identified that supports new NRC application requirements

The current specifications for NRC's personal computers are:

Hardware:

Standard PC: 500Mz, 8.4 GB HD, 128 DIMM SDRAM, 19" monitor.

Software:

Core: Corel WordPerfect Suite 8.0, Windows NT 4.0, GROUPWISE 5.0, Novell NetWare Suite, Norton Virus Control, Netscape, CITRIX Web-based Applications, Agency Documents Access and Management System (ADAMS)

Additional: Microsoft Word, Excel and PowerPoint.

Desktop Services. Maintenance of the business applications microcomputer inventory for the Headquarters Office. This includes maintaining basic desktop workstations and peripheral equipment that support NRC staff at their primary work locations, and includes the high performance workstations.

Desktop systems support functions for the Headquarters Office include installations of new software and hardware, system relocations, routine maintenance, back-ups, data and system restorations, documentation, security, and technical services.

Non-Infrastructure Acquisitions. Acquisition and installation of special purpose workstation hardware and software for the Headquarters Office. Provide for acquisition and installation of non-infrastructure workstation hardware and software requested and funded by offices, including such items as engineering workstations, portable computers, scanners, tape drives, printers, non-standard monitors, memory, CD-ROMs, special software, and larger hard drives.

2.1 Maintenance

2.1.1 Hardware Maintenance

- Perform Tier 2 troubleshooting and diagnostics to ensure that all supported hardware is performing in accordance with service level requirements.
- Identify failing hardware and restore to service in accordance with service level requirements.
- Install upgrades, modifications, and maintenance releases in accordance with service level requirements, including engineering changes, maintenance updates, and upgrades.
- Perform preventive maintenance in accordance with service level requirements, including engineering changes, maintenance updates, and upgrades.
- Maintain service/repair logs for each supported hardware system and its components.

2.1.2 Spare Parts

- Provide an on-site stock of spare parts and components needed for the repair of all maintained hardware.

2.1.3 Special Maintenance

- Provide special maintenance as requested.

1.4 Software Maintenance

- Perform Tier 2 troubleshooting and diagnostics to ensure that supported software is performing in accordance with service level requirements.
- Identify failing software and restore to service in accordance with service level requirements.
- Install maintenance releases in accordance with service level requirements, including engineering changes, maintenance updates, patches, and upgrades.
- Perform preventive maintenance in accordance with service level requirements, including engineering changes, maintenance updates, patches, and upgrades.

2.1.5 Diagnostic Utilities

- Perform hardware and software diagnostics as appropriate to maintain service levels.

2.1.6 Warranties

- Ensure compliance with supported hardware and software license and warranty restrictions.

- Register hardware and software as necessary with vendors in order to receive notices and maintenance updates.
- Keep and maintain warranty service and repair logs for each hardware and software license.
- Track warranties to ensure compliance.
- Adhere to and enforce vendor warranty contracts and agreements.

2.1.7 Reporting

- Summarize all system down times and problems and current status in the weekly report and attach a copy of the system trouble logs.

2.2 Installation/Deployment

2.2.1 CSC Service Requests

- Install new desktop system components, relocate desktop components, install upgrades, modifications, and peripherals in response to approved CSC Service Requests.
    - Provide integrated, working, and tested systems with configurations that comply with NRC standards and specifications.
    - Schedule installations i
    - Perform pre-install walk-through to prevent move-related problems.
    - Deliver, set-up, and test installations.
    - Establish system and application functionality and connectivity after installation.
    - Installation is complete when all applications, including those requiring network access, are installed and working to the satisfaction of the user.
    - Deinstall, remove and dispose of surplus, failing, or obsolete hardware and software according to NRC procedures, as requested

2.2.2 Network Coordination

- Coordinate with the network support vendors prior to system installation to ensure that the network software and hardware is properly configured to support and recognize the new system, using established coordination and communication procedures.

2.2.3 Hardware Coordination

- Ensure that the electrical power and network connections are working.
- Coordinate with the facilities, electrical, and cabling vendors prior to delivery, to ensure that the site is prepared.
- Provide furniture or cabinets as required, with NRC approval.

2.2.4 Software Coordination

- Ensure that original system software image and customer data is preserved (backed up) prior to commencing work so that the system can be restored to its original state if necessary.
- Perform minor customization and integration modifications of the systems as necessary to maintain continued operations after installation.
- Ensure that modifications are in compliance with NRC configuration standards.

2.3 ADAMS Support

The NRC Agencywide Documentation And Management System (ADAMS) is a significant initiative currently underway at NRC. ADAMS is an electronic document and records management system that maintains NRC's unclassified official program and administrative records in a centralized electronic document repository. The major components of ADAMS include FileNet's Integrated Document Management software and other related applications that are integrated and operate in Windows NT, Novell, and GroupWise environments.

For ADAMS, ITID provides the following Operations and Maintenance support:

- Maintain ADAMS document entry workstations
- Maintain ADAMS servers
- Develop and run reports on ADAMS system use, performance and availability
- Provide ADAMS Training Services through the CSC

Other OCIO organizations provide user training and assistance in performing the following document management tasks: data entry; document entry; indexing documents; setting access privileges for documents; retrieving documents; printing of documents; electronic distribution of documents; electronic signatures on documents; archiving documents; and document scanning functions

- Provide Tier 2 customer support for ADAMS software and equipment including.
  - Document entry
  - Indexing
  - Security
  - Retrieval
  - Printing
  - Distribution
  - Electronic signatures
  - Archiving

- Document Management

- Provide Tier 2 ADAMS Administration support including:
  - Develop and run reports
  - Troubleshoot problems
  - Define and maintain user and group profiles
  - Manage searches
  - Provide support for logins/passwords
  - Monitor system logs
  - Assist in the reclaim process
  - Assist in establishing and maintaining:
    - User naming conventions
    - Libraries
    - Folders

- Develop and maintain work flow in a Novell GroupWise, Microsoft NT, and ADAMS/FileNET environment.

- Provide on the job training to others as needed.

- Create/update records in NRC's tracking system and in other systems.

- Participate in information gathering, technical problem studies, and evaluation of software and hardware as needed.

- Become knowledgeable of and perform work within the guidelines of established NRC policies and procedures pertaining to ADAMS.

2.4 Non-Infrastructure Acquisitions

- Provide for acquisition and installation of non-infrastructure workstation hardware and software requested and funded by offices, including such items as engineering workstations, portable computers, scanners, tape drives, printers, non-standard monitors, memory, CD-ROMs, special software, and larger hard drives.

2.5 Procurement

2.5.1 Hardware/Software

- Order hardware and software accordance with service level requirements.

- Order hardware and software maintenance releases, including engineering changes, maintenance updates, fixes, and upgrades.

- Arrange for maintenance agreements and support from hardware and software providers as appropriate.

- Purchase hardware and software diagnostic utilities as appropriate to maintain service levels.

2.5.2 Spare Parts

- Purchase and spare desktop system parts and components needed to assure continued operation of supported hardware.

3 NETWORK SERVICES

The current NRC IT Infrastructure Architecture provides an Agencywide standard method for delivering IT services to the desktops of NRC employees and designated Contractors; and facilitating communications with external organizations such as other domestic and foreign government agencies, nuclear power plants, laboratories and the general public.

Network Services administration and operational support functions include installation, troubleshooting, diagnostics, operation, maintenance, management, and administration of the NRC data, voice, and video communications infrastructure. Network services provide NRC users with shared network storage, network printers, E-Mail, Internet and Intranet browsing services, remote applications connectivity, and nationwide access to Agencywide applications.

The Network Services *Information Technology Architecture* Report dated September 13, 1999, and an NRC network equipment inventory list, *List of Equipment,* is provided in Section J to provide further details on the NRC Network.

3.1 Network Operations Center (NOC)

The NRC Network Operations Center (NOC) operates and maintains services Agencywide to monitor network operations, track network performance, and troubleshoot problems to restore degraded network hardware, and applications software elements to service. The NOC is also responsible for scheduling, coordinating and implementing all upgrades to equipment and software associated with network services. The NOC uses state of the art network tools such as Optivity and Openview are used to monitor and maintain the infrastructure, E-mail services, IP services and application services.

Network component systems include: hubs, routers, communication links, Regional links, and all other supporting data communications for NRC's Network operations. Also included are systems that primarily support the Network infrastructure, including: network servers, file servers, message (E-Mail) servers, gateway servers, web servers, bastion hosts, and firewall systems.

HQ workstations are connected to an Ethernet local area network (LAN). Each NRC location uses the same architecture for its LAN installations. The Agency's computer centers, including its servers and mini-computers, are connected to the NRC Headquarters backbone network via . External networks, Internet services, and timesharing services are also connected to the NRC backbone network utilizing cyber security systems such as firewalls.

- Identify, evaluate, develop and implement network management processes and procedures from an operational support perspective to perform proactive fault management, performance management, growth management, and security management for all network components, systems, and services

- Implement and operate network services performance measurement systems to provide periodic reports to NRC management on network services performance relative to the NRC customer service level requirements and service level agreements.

- Plan and manage network growth by predicting future trends based on historical network trends and business information

3.2 Current NOC Operations

- Operate the network during designated hours and monitor availability and performance.
- Operate the network to provide consistent operation and optimum performance.
- Provide the NOC Monthly Security Report
- Provide operational support for E-mail and Internet server applications administration, systems programming support, database administration, hardware/software configuration, and inter-system communications.
- Perform integration testing and approve new Desktop PC hardware, software, and peripheral systems for installation into the network infrastructure Production Operations Environment (POE).
- Procure, integrate, test, and coordinate installation of network-related hardware and software on Desktop PC systems, such as NetWare and Citrix clients, network interface cards, network printer drivers, etc.
- Provide and maintain an automated software distribution system for the software installed on Desktop PC's and network servers.
- Provide network availability and response according to NRC service level requirements.
- Perform diagnosis, identification, and correction of failing network components or failure of the interfaces between network components and other systems, operating environments, or applications.
- Use tools to remotely identify and diagnose network problems.
- Monitor availability and status of network systems.

3.2.1 Network Management

- Identify, evaluate, develop and implement network management from an operational support perspective to perform proactive fault management, performance management, growth management, security management, asset management, for all network components, systems, and services.
- Identify and implement metrics and thresholds to measure and manage fault, growth, performance, security, and accounting for the network using automated network tools.
- Measure performance of network components for compliance with manufacturer's published performance specifications for network hardware and software.
- Gather and analyze network and desktop statistical information and provide recommendations to improve network performance.
- Identify and resolve problems proactively before they affect users in order to ensure high network availability and reliability.

- Consolidate network tools into an integrated network management system.
- Maintain and operate network tools which are available for the routine operation and maintenance and monitoring of network components, services and systems.
- Provide operational support for network tools during the development of new technology to ensure maintainability and supportability of new technology.
- Review the current network tools and make recommendations for their enhancements or replacement.
- Develop and implement new capabilities to perform the required network management functions based on the implementation of new technology.
- Plan and manage network growth by predicting future trends based on historical network trends and business information.
- Monitor and manage network traffic patterns and identify issues such as "bottlenecks" that may reduce performance.
- Provide routine reports on system status and availability of network components, systems, and services.
- Monitor and manage in realtime the availability of network components, systems, and services for optimum performance and availability.

3.2.2 CSC Service Requests

- Work closely with and support the Help Desk Contractor in resolving user problems related to the network infrastructure, LAN logon and User ID administration, file security, and security services, including network failures or failures of network interfaces to other systems.
- Work closely with and support the Desktop PC maintenance Contractors in resolution of Desktop PC software and hardware problems. Respond to requests for assistance from the Desktop PC maintenance Contractors. Support Desktop PC refresh activities.
- Work closely with and support the Cable Plant and Telecommunications Contractors in resolving user problems related to network infrastructure systems or requiring diagnostics from network infrastructure management systems.
- Dispatch appropriate maintenance personnel to resolve the CSC Service Request.
- Record observations and conclusions on CSC Service Requests.
- Monitor progress until problem is resolved.
- Provide CSC periodic status reports on CSC Service Requests and respond to status inquiries from CSC.

3.2.3 Failures

- Identify and resolve problems proactively before they affect users in order to ensure high network availability and reliability
- Respond to all reports of network failures or failures of network interfaces to other systems.
- In the event of a failure, take immediate corrective actions to restore the network to service.
- In the event of a failure notify the CSC of the expected time to repair and return the network to service.

3.2.4 Service Provisioning

3.2.4.1 Remote Access System

- Perform order entry activities for Remote Access System dial-up phone lines from the appropriate telecommunications service provider for headquarters and regional offices as required.
- Place requests for moves, additions and changes to existing remote access dial-up phone lines.
- Confirm receipt of new services, service changes or disconnect orders for remote access dial-up phone lines.

3.2.4.2 Resident Inspector Sites Frame Relay Connections

- Perform order entry activities for frame relay connectivity from the appropriate telecommunications service provider for headquarters, regional offices and resident inspector sites as required.
- Place requests for moves, additions and changes to existing frame relay services and connections.
- Confirm receipt of new services, service changes or disconnect orders for frame relay connections.

3.2.4.3 WAN Connectivity

- Perform order entry activities for WAN connectivity from the appropriate telecommunications service provider for headquarters, regional offices and resident inspector sites as required.
- Place requests for moves, additions and changes to existing WAN services and connections.
- Confirm receipt of new services, service changes or disconnect orders for WAN connections.

3.2.5 On-call Operations

- Provide support for extenuating events outside normal operational periods as required to maintain network systems.

3.3 Maintenance

3.3.1 Hardware Maintenance

- Perform required maintenance on all network hardware.
- Install upgrades, modifications, service releases, and maintenance releases for network hardware, including engineering changes, maintenance updates, patches, and upgrades.
- Perform preventive maintenance on network hardware, including engineering changes, maintenance updates, patches, and upgrades.
- Maintain network hardware service and repair logs for all network systems which will record system down times, problems, causes, resolution, and status.

3.3.2 Spare Parts

- Provide an on-site stock of spare parts and components needed for the repair of all network hardware.

3.3.3 Software Maintenance

- Provide maintenance of all supported network software.
- Install upgrades, modifications, service release, and maintenance releases to network software as necessary to meet the service levels and refresh intervals, including engineering changes, maintenance updates, patches, and upgrades.
- Perform preventive maintenance on network software as necessary to meet the service levels and refresh intervals, including engineering changes, maintenance updates, patches, and upgrades.

3.3.3.1 Warranties

- Ensure compliance with network hardware and software license and warranty restrictions.
- Register network hardware and software as necessary with vendors in order to receive notices and maintenance updates.
- Keep and maintain warranty period, service, and repair records for each network hardware and software license.
- Adhere to and enforce vendor contracts warranties and agreements on network hardware and software.

3.3.4 Special Maintenance

- Provide special maintenance as requested.
- Respond to special maintenance requirements at Regional and other NRC offices.

3.3.5 Reporting

- Summarize network hardware service and repair logs including current status in the weekly report and attach a copy of the system trouble logs.
- Notify NRC immediately when any system goes down or is malfunctioning.
- Provide reports on the performance and availability of LAN and WAN cable, telecommunications, and desktop systems.

3.4 Installation/Deployment

3.4.1 New Systems

- Provide configuration, integration, installation and operational support and administration for network components, network connectivity, and software distribution for new agency systems, services, and business applications.
- Validate system functionality and connectivity after installation, following NRC policies and procedures for installations.

3.4.2 Relocations

- Relocate network systems in accordance with validated move requests.
- Schedule network moves in accordance with NRC policies, procedures and service level requirements.
- Re-establish system functionality and connectivity after moves, following NRC policies and procedures for installations.

3.5 Procurement

3.5.1 Hardware/Software

- Order hardware and software maintenance releases in accordance with NRC policies, procedures and service level requirements, including engineering changes, maintenance updates, fixes, and upgrades.
- Arrange for maintenance agreements and support from hardware and software providers as appropriate.
- Purchase hardware and software diagnostic utilities as appropriate.

3.5.2 Spare Parts

- Purchase and stock spare desktop system parts and components as needed.

3.6 Regional LAN Administrator Support

- Provide first and second level Regional LAN Administrator Support to maintain and support the network including:
  - Hardware
  - Software application problems
  - Analyzing and resolving from a total systems perspective desktop, software and networking problems including:
    - Providing password resets
    - LAN disk space allotment
    - Network printer configuration
    - Operating, monitoring, and administering network components, associated peripheral equipment, and the overall network environment
    - Performing daily backups of file servers and applications servers
    - Identifying, troubleshooting, answering questions, and resolving problems for COTS software applications.

POSITION DESCRIPTION

Position: COOP LAN Administrator

Functions: Monitor, install, integrate, operate, maintain, and support the servers, workstations and printers, associated peripheral equipment, and network environment. Provides user specific support such as troubleshooting and solving software problems, and determining hardware problems (e.g., Printing, NIC cards, WordPerfect). Recognizes problems and requests assistance. Communicates effectively with end-users, technical support staff and management. Provides status reports regarding operational problems, issues, failures, and outages. Update and maintain operational system documentation and standard operating procedures.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science or a related field. Five (5) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

Three (3) years experience as a Novell or NT LAN Administrator is required, and technical knowledge of UNIX LAN and LAN/WAN operations is desired. This position requires a sound knowledge of local area networks, network security, routing protocols, and office automation systems. It requires previous experience and ability in providing technically sound hardware and/or software solutions to meet various NRC requirements. It also requires the ability to deal effectively with NRC personnel.

POSITION DESCRIPTION

Position: Regional LAN Administrator

unctions: Provides user specific support such as troubleshooting and solving software problems, and determining hardware problems (e.g., Printing, NIC cards, WordPerfect). Operates, monitors, installs, and administers servers, workstations and printers, associated peripheral equipment, and network environment. Recognizes problems and requests assistance. Communicates effectively with end-users, technical support staff and management.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science or a related field. Five (5) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

Three (3) year experience as a Novell or NT LAN Administrator is required, and technical knowledge of UNIX LAN operations is desired. This position requires a sound knowledge of local area networks and office automation systems. It requires previous experience and ability in providing technically sound hardware and/or software solutions to meet various NRC requirements. It also requires the ability to deal effectively with NRC personnel.

POSITION DESCRIPTION

Position: ADAMS System Administrator

inctions: Provide client support and systems administration for ADAMS, including software installation, configuration, administration, and support for Saros, Ensemble, Panagon/Mezzaine, @Mezzaine, Watermark, IQ-Objects/Report Manager, Foremost, and other related software (e.g., Internet software, etc.) at the desktop and scanning stations. Perform some server level processes (e.g. Fileshare functions).Provide support for document entry, indexing, retrieval, printing, distribution, archiving, management, and scanning (including Watermark Workstation Administration). Develop and run reports; test and evaluate software; troubleshoot problems; define and maintain user and group profiles; manage searches; provide support for logins/passwords; assist in the reclaim process; assist in establishing and maintaining user naming conventions and folders; and develop and maintain work flow in a Novell GroupWise, Microsoft NT, and FileNET environment.

The specific software packages and versions used may change over time.

Create and maintain local operating and quality assurance procedures and develop recommendations for revising business processes where possible. Provide client support services and procedural assistance to users and assist in the development of training materials. Provide on the job training to others as needed. Process scanning requests and security authorization forms, and carry out other activities. Participate in information gathering, technical problem studies, and evaluation of software and hardware as needed.

Skills:

- Strong analytical skills
- Good organization skills

- Ability to provide first level support in a courteous and professional manner
- Ability to effectively communicate verbally and in writing
- Ability to work independently or as a team leader or member as required
- Ability to install and configure software
  Ability to perform system administration functions

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science or a related field. Five (5) years directly related experience in the networking field may be substituted for the educational requirement. Certification or completion of substantial training in a related personal computer, network, or imaging field may be substituted for part or all of the above requirement.

Experience:

A minimum of five (5) years system configuration, administration, or support experience in an automated imaging or other complex computing environment such as Microsoft NT or Novell environment is required for this position. Three years must be specialized experience as a Novell or NT LAN Administrator. The remainder may be specialized or general experience.

This position requires three years of FileNET administration or support experience, or the satisfactory completion of FileNET training.

POSITION DESCRIPTION

Position: High Performance Computing LAN Administrator

Functions: Operate, monitor, and administer high performance workstations, servers and associated peripheral equipment, and network environment. Integrate and ensure operability of applications and scientific codes into the high performance computing environment. Provides user specific support such as troubleshooting and solving software problems, and determining hardware problems. Communicates effectively with end-users, technical support staff and management. Coordinates high performance computing equipment maintenance. Provides status reports regarding operational problems, issues, failures, and outages. Updates and maintain operational system documentation and standard operating procedures.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, mathematics, engineering, accounting or business administration or a related field. Five (5) years directly related experience in high performance computing field may be substituted for the educational requirement.

Experience:

Technical knowledge of LAN/MAN/WAN operations and UNIX environments is required. Five (5) years hands-on experience as a UNIX LAN Administrator is required, and technical knowledge of high performance computing operations is desired. It requires previous experience and ability in providing

technically sound hardware and/or software solutions to meet various NRC requirements. It also requires the ability to deal effectively with NRC personnel.

4 INFRASTRUCTURE DEVELOPMENT AND IMPLEMENTATION SERVICES

IT Infrastructure Development and Implementation Services provide for the **development, integration, and implementation** of all information technology infrastructure resources including desktop systems, local and wide area network systems, high performance desktop and network systems, telecommunications, video-telecommunications, and Data Center, and other related Tier 3 technical support.

4.1 Systems Engineering

Infrastructure Development and Implementation Branch (IDIB) performs as an overall NRC IT infrastructure architectural engineer, providing strategic recommendations, planning, coordination, design, development, testing, and integration for all NRC IT infrastructure projects, systems, applications, and future requirements.

4.1.1 IT Infrastructure Development

IDIB develops a comprehensive IT Infrastructure architectural strategy to meet the changing mission requirements of the NRC and to maintain compliance with service level requirements. IDIB develops the short and long range plans necessary to implement the strategy. IDIB provides specific system requirements for additions, changes, upgrades and deletions to the applications and equipment necessary to implement the strategy.

4.1.2 IT Infrastructure Integration

IDIB provides all technical services needed to integrate changes to the applications and equipment of the NRC IT Infrastructure Production Operations Environment (POE). The life-cycle of required developmental/integration activities includes, but is not limited to development and/or refinement of functional requirements; analysis of alternative conceptual designs; test and evaluation of pilot systems; demonstration of new capabilities to NRC end-users; integration of new capabilities with existing network hardware and software products; development of implementation plans including costs estimates, scheduled rollout, resources required, etc.; training of contractor personnel; training of NRC staff (but not end users); training plans for NRC end users; and operational cut-over plans.

Examples of development and integration projects include, but are not limited to:

- Workstation application or equipment upgrades or changes
- Revision of Workstation images
- New Workstation scripts
- New NT upgrades
- Network server application or equipment upgrades or changes
- Unix workstation or server application or equipment upgrades or changes
- New firewall appliances, proxy servers, and caching devices

4.1.3 IT Infrastructure Implementation

IDIB provides testing, network performance impact analysis, network modeling and simulation, integration, demonstration, product briefings, evaluation, and orientation/training. As part of this activity, comparison of alternative solutions and determination of the most cost-effective configurations and implementation

alternatives to meet end-user needs is performed.

4.2 IT Infrastructure Services

4.2.1 Workstation System Services

IDIB provides life cycle development and integration services for the NRC workstation image which is deployed Agency-wide on all NRC workstations. Elements to be supported include the operating system, standard office automation applications such as E-mail, scheduler/calendar, word processor, spreadsheet, presentation graphics, web browser, the upgrade to a new office automation suite, support for multi-media, network connectivity, local and network printers, drivers, and utilities etc. Also included is a requirement to support the development and upgrade of workstation and peer server/workstation configurations at the NRC's resident inspector sites, special remote computing workstations, laptop systems and docking stations.

4.2.2 Local and Wide Area System Services

4.2.2.1 Infrastructure Services

IDIB provides life cycle development and integration services for all development efforts related to NRC Local and Wide Area Network projects. Elements to be supported include Network hubs, switches and routers; Internet connectivity; WAN connectivity to remote locations (regions, resident inspector sites, LABS, NIH, etc.), remote/dial-up access; video teleconferencing; video streaming; video consolidation, Virtual Private Networks (VPNs), and audio telecommunications systems. Also included is (1) development of related hardware and software, and (2) a capability to manage connectivity and monitor services used on each infrastructure device circuit or virtual circuit.

4.2.2.2 Web Architecture Services

IDIB supports the Web Architecture environment at the NRC. Elements supported include Unix and NT servers, Netscape/iPlanet and IIS Web servers, Tuxedo and ColdFusion application environments, LDAP compliant directory, and Sybase and SQL/Server DBMS. IDIB develops and implements the web site infrastructure to support end-user development, configuration of the web server to enable Secure Sockets Layer, establishes a three-tier architecture using ColdFusion in the middle tier, develops application server platforms to include a Web Publisher platform including publishing rules, engineers a framework for utilizing LDAP-compliant directory with a three-tier security implementation, and creates a distributed content management framework to support end-user development with authoring tools available for use by program offices.

4.2.2.3 LAN/WAN Server Services

IDIB provides life cycle development and integration services for all IT Infrastructure file, application, remote computing, printer, Web and other servers. Support required includes responsibility for development and enhancements of all component parts of the physical hardware platform, storage systems and media, operating systems, backup systems, CD storage systems, UPS's, groupware, client drivers, NDS and server management utilities, and any other ancillary devices and applications associated with these servers.

4.2.3 High Performance Computing Environment (HPCE) Services

IDIB provides HPCE workstation and server systems life-cycle development and integration services. Elements supported include the applications (unique, or vendor supplied scientific code), operating systems, physical hardware platforms, storage systems and media, the backup systems, CD storage systems, network printers, UPS's, client drivers, server management utilities, and any other ancillary devices and applications associated with these workstations and servers. IDIB is responsible for assisting nuclear engineers with troubleshooting scientific code integration issues if they do not run properly within the NRC environment. The servers are primarily located in three separate rooms that support the Program Offices and consist of mostly Unix servers and workstations. IDIB is responsible for coordinating server installation and repair as needed with vendors under the terms of purchase or hardware/software support contracts. Duties include configuration of COTS software, management of license key generators, support for printer and plotter driver integration and analysis and management of memory performance based on statistics. Support also includes mail routing troubleshooting, database migration efforts, management of tape backup scripts and running of special tape backups, modification of directory structures, and assisting users with file transfer protocol problems as well as the installation of SQR, COBOL, C, and other languages and compilers as required.

4.2.4 Other IT Infrastructure Services

4.2.4.1 IT Infrastructure Security Services

IDIB provides life cycle development and integration services for IT infrastructure and workstation security. This includes providing protection from both external and internal sources and allows a working balance of available services and reliable security. Support required includes responsibility for development and enhancements of all component parts of Internet firewalls, e-mail systems, intrusion detection systems, web servers, network management systems, Dynamic Host Configuration Protocol (DHCP) capabilities, audit trail and alert capabilities, Electronic Commerce, Electronic Information Exchange, public access, virus protection, digital certificates, digital signature capabilities, and the monitoring of Computer Emergency Response Team (CERT), Computer Incident Advisory Capability (CIAC), and European Organization for Nuclear Research (CERN) security bulletins, as well as the daily review of firewall, and Intrusion Detection System (IDS) logs using appropriate scripts and native operating system commands in search of anomalies and responding to them and notifying the NRC. IDIB reviews and analyzes the logs and prepares a monthly report on Internet intrusion attempts. IDIB responds to hacker break-ins, assists with the conduct of independent security audits, analyzes security filtering/functionality problems, responds to security threats like the Berkeley Internet Name Domain (BIND) vulnerability, and tests and maintains Sendmail and IDS RealSecure software at current versions.

4.2.4.2 Contingency Management

IDIB develops/reviews and updates if necessary, the contingency management plans to support the NRC IT Infrastructure in the event of a loss of primary or critical IT infrastructure services; designs, plans, and implements as necessary, the components required to support the NRC IT infrastructure in the event of a loss of primary or critical IT infrastructure services; provides support in performing recovery operations in the event of a catastrophic network failure, loss of critical network elements, and/or for purposes of testing of the contingency systems/plans; performs semiannual audits of compliance with NRC disaster recovery procedures; responds to reports generated from independent audits of procedure compliance; and supports disaster recovery site (s) to ensure viability of recovery at remote sites in the event of a HQ disaster.

4.2.4.3 Procurement

IDIB procures services, support, hardware and software for NRC prototype and production systems to support the design, development, integration, and implementation of NRC applications or equipment. Procured products include, but are not limited to: desktops, laptops, printers, and network components such as: servers, hubs, routers and other auxiliary components connected to the network.

4.3 Development, Integration, and Implementation Life-Cycle

The NRC has implemented the Infrastructure Development Process Model (IDPM) as the standard life-cycle methodology for release management of new technology to the Production Operation Environment (POE), or modifying existing systems within the POE. In introducing NRC applications into the NRC POE, the "Development Process Model (DPM)" is followed. It ensures that the development and/or integration tasks 1) result in effective design, testing, and integration of applications that pass production testing, 2) are integrated into production without adverse impact on the POE, and 3) perform as designed. The number and scope of DPM activities vary from project-to-project based on the degree of complexity.

All development/integration projects generally include the stages described below.

4.3.1 Detailed Requirements Analysis

- Analyze new NRC requirements, industry trends, and technology advances related to NRC network and workstation infrastructure.
- Provide requirements analyses, needs assessments, recommendations and business cases for system upgrades, design modifications, and additional capabilities.
- Meet with NRC users and technical staff to define the users' requirements.
- Determine impact of new development on production environment.
- Make a determination of project feasibility.

4.3.2 Design

- Develop conceptual and detailed system designs.
- Identify the technical teams involved in design and development.
- Create detailed functional specifications.
- Prepare a detailed conceptual design.
- Obtain approval of the functional specifications and conceptual design by the NRC.
- Prepare one or more technical designs.
- Prepare an integration plan, with product specifications, project schedule, resource requirements,

budget estimates, and option comparisons.

- Conduct a technical review.

4.3.3 New Technology Development

- Develop new systems, system upgrades, and automated upgrade processes based on the technical designs.
- Purchase, assemble, and/or build the components and systems.
- Perform custom integration as required.
- Make changes to the technical design, as needed.
- Develop the tools needed to be added or modified in the Integrated Network Management System (INMS) to provide management and automated monitoring of the new technology and to provide the data required for reporting.
- Prepare a user guide and any changes required of the detailed design document and technical specifications.
- Prepare the support, operations and maintenance plan for the new technology.
- Prepare and obtain approval of a comprehensive test plan based on the functional specifications.

.3.4 New Technology Acceptance Testing

- Conduct a stakeholders review of the Acceptance Test Plan.
- Operate a network test laboratory and staging facility to support network related testing, network performance analysis, modeling and simulation and staff orientation.
- Conduct internal testing, in an isolated controlled environment (test lab).
- Develop conceptual and detailed plans for testing and evaluation of pilot IT infrastructure capabilities, and to demonstrate new capabilities.
- Conduct progression/regression testing to ensure that new IT infrastructure products or systems do not adversely affect the existing and future production operations environments.
- Coordinate testing with applications support personnel.
- Perform user tests to assure that the systems/upgrades will meet the needs of NRC staff per the original analysis.
- Conduct load and stress, functionality, and other tests as defined in the Acceptance Test Plan.

- Document and publish test results.

4.3.5 Transition to Production Operational Support

- Complete any outstanding documentation, and any outstanding final approvals.
- Develop and execute operational cut over plans.
- Train the NOC and CSC staff members in installation and support of the new technology.
- Integrate lessons learned into documentation and product, with NOC and CSC staff participation in finalizing any document or new technology changes.
- Obtain approval of the final implementation schedule.
- Purchase the necessary hardware and/or software licenses required for Agency-wide rollout.

4.3.6 Implementation

- Work with Network Operations Center and Customer Support Center to implement new products.
- Provide on-call telephone and on-site assistance to the NOC and Customer Services Center during implementation and as a secondary level of operational support.
- Provide support for restoration of prior configurations if necessary to maintain operational integrity.

.3.7 Position Descriptions

Beginning on the following page and continuing through the remainder of the section are the position descriptions the Contractor is required to fill. Not all positions must be filled at all times. All key positions shall be filled at the initiation of activities under this contract. In addition, certain additional positions shall be directed by the NRC to be filled. Other positions (e.g., consultants) shall be filled only during certain times and with the direction of the NRC. The position descriptions are a catalog of skills the Contractor will be required to provide.

4.3.7.1 LAN Administrator

POSITION DESCRIPTION

Position: LAN Administrator

Functions: Provide user specific support such as troubleshooting and solving software problems, and determining hardware problems (e.g., Printing, NIC cards, WordPerfect). Operates, monitors, and administers servers, workstations and printers, associated peripheral equipment, and network environment. Maintains scheduled reports of LAN/WAN operations activities. Recognizes problems and requests assistance. Administrates system user accounts.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science or a related field. Five (5) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

Four (4) years experience as a Novell or NT LAN Administrator is required, and technical knowledge of UNIX LAN operations is desired. This position requires a sound knowledge of local area networks and office automation systems. It requires previous experience and ability in providing technically sound hardware and/or software solutions to meet various NRC requirements. It also requires the ability to deal effectively with NRC personnel.

4.3.7.2 LAN Systems Analyst

POSITION DESCRIPTION

Position: LAN Systems Analyst

Functions: Provides Novell and/or Windows expertise.

Performs activities associated with design and implementation of local area networks and office automation systems. Analyzes, designs, integrates documents, implements "state of the art" local area network, office automation and microcomputer systems applications. Performs comparative analyses of commercial software packages. Conducts scientific and statistical analyses. Conducts user and technical training guidance for the NRC. Assists local area network analysts and programmers with planning, organizing, controlling, and scheduling of activities.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, mathematics, engineering, statistics, operations research, accounting or business administration. Five (5) years directly related experience in the networking field may be substituted for the educational requirement. If the position is for a Novell product, the individual shall be a Certified Novell Engineer (CNE) or have equivalent on-the-job experience. If the position is for a Microsoft product, the individual shall be a Microsoft Certified Systems Engineer (MCSE) or have equivalent on-the-job experience.

Experience:

At least five (5) years of experience with progressively more difficult LAN/network responsibility and with a minimum of three (3) years of systems analysis, to include work as an analyst for complex office automation and local area network systems. This position requires a sound, thorough, practical and theoretical knowledge of local area networks and office automation systems. It requires previous experience and ability in providing technically sound hardware and/or software solutions to meet current and expanding Novell and/or NT and network requirements. It also requires initiative, imagination, analytical ability, and the ability to deal effectively with NRC personnel.

4.3.7.3 Network Analyst

POSITION DESCRIPTION

Position: Network Analyst

Functions: Major participant in all network discussions ranging from problem definition through problem solution of major projects. Works with minimum supervision. Prepares substantial parts of interim and final reports. Often assigned more than one task at a time, and therefore, must be capable of effectively planning the use of time and must be able to divide time among several tasks. Generally has extensive contact with NRC staff. Generally designated as project leader of a small to medium sized project or a portion of a larger one. Performs services as a technical expert in one or more of the following areas:

Local and wide area network planning, design, testing, integration and engineering.

Qualifications:

Education:
Bachelors level degree from an accredited university or college is required in telecommunications, electrical engineering, computer science or related fields. Six (6) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:
At least five (5) years of experience with progressively more difficult LAN/network responsibility in design of wide area network, office automation and network systems is required. This includes 2 years in design of wide area networks, and office automation systems, telecommunications systems and 1 year in network management. This position requires good analytical and problem solving ability, creativity and insight. Requires skills in verbal and written communications.

4.3.7.4 Security Analyst

POSITION DESCRIPTION

Position: Security Analyst

Functions: Performs activities associated with the implementation and support of security systems on the Local and Wide Area Network services in Novell, NT and UNIX environments, and between that network and the Internet. Evaluates, installs, customizes and integrates commercial and custom security applications and hardware. Programs specialized applications as necessary to meet security requirements.

Implements and maintains security "firewalls" between networks, especially between NRC networks and the Internet.

Conducts user and technical training, and provides guidance in the operation and use of security applications throughout the NRC environment.

Provides trouble shooting and problem resolution for Novell, NT and UNIX security applications.

Assists other staff and programmers in the security aspects of design, development and implementation. May act as project manager.

Maintains liaison with the security community in order to obtain the most current security advisories and otherwise remain current on security matters and to keep the NRC security system current.

Performs the analysis and design of automated systems/subsystems requirements with particular emphasis on security matters such as encryption, verification and authentication. Develops programs, C-shell scripts, and other work for the implementation of security systems for network applications.

Qualifications:

Education:

Bachelors level degree from an accredited university or college in computer science, mathematics, engineering, accounting or business administration is required. Six (6) years directly related experience as a security programmer of which at least two years were as a security analyst may be substituted for the educational requirement.

Experience:

Minimum five (5) years of ADP experience, preferably three years programming experience and two year experience in problem analysis and/or system design. This position requires a minimum of two (2) full years of sound, thorough, theoretical and practical knowledge of security systems and related programming gained through experience. Specific experience is desirable with network security (UNIX security experience mandatory), firewalls, Internet security and network protocols. This position requires previous experience and ability in providing technically sound hardware and/or software security solutions to meet current and expanding network requirements. Position also requires initiative, imagination, analytical ability and the ability to deal effectively with NRC personnel. Previous work with federal government agencies is desirable.

4.3.7.5 Senior Systems Architect/Engineer

POSITION DESCRIPTION

Position: Senior Systems Architect/Engineer

Functions: Provides technical support to the NRC long range plans for network upgrades and enhancements. Works with users and staff to develop requirements and to analyze and recommend alternative approaches to meet those requirements.

Performs activities associated with the design and implementation of local and wide area networks and office automation systems. Analyzes, designs, integrates documents, implements "state of the art" local and wide area networks, office automation systems and microcomputer systems and applications. Performs comparative analysis of commercial software packages. Conducts scientific and statistical analyses. Conducts user and technical training. Assists LAN Analysts and programmers in the planning, organizing, controlling and scheduling of activities. May act as project manager.

Serves as the technical expert in the area of measurement and analysis of LAN, WAN, and OFFICE AUTOMATION systems hardware and software. Measures and reports on the performance of LAN, OFFICE AUTOMATION, ADP, and telecommunications systems. Maintains the performance database,

performs performance analysis to identify and seek solutions to performance problems.

Provides administrative and technical consultation on a wide variety of management concerns such as: office and automation studies, system and processing problem areas, areas for potential improvement, and methods and procedures to promote the efficiency and effectiveness of office systems operations. Provides guidance and management analysis capabilities to resolve processing and office system operation problems.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, electronics, mathematics, engineering, statistics, operations research, accounting, business administration, or computer related field is desirable. Ten (10) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

At least ten (10) years experience with progressively more difficult LAN/network responsibility including a minimum of eight (8) years of systems analysis including acting as lead analyst for development of LAN, WAN and OFFICE AUTOMATION systems. This position requires a sound and thorough theoretical and practical knowledge of LAN, WAN and office automation systems. Requires skills in verbal and written communications. It also requires initiative, imagination, analytical ability, and the ability to deal tactfully and effectively with customers and NRC network staff. Previous work with federal government agencies is desirable.

4.3.7.6 Senior Systems Consultant

POSITION DESCRIPTION

Title: Senior System Consultant

Functions: Serves as senior technical advisor on complex projects as determined by the Contractor or requested by the NRC. May serve as team leader on difficult or significant projects. Provides technical expertise when assigned to a project. May be required to participate in any phase of major project from concept definition through implementation and support. May be assigned to several concurrent tasks. Will have close contact with customers at all levels of the NRC. Provides expertise in the following areas:

1. Integration of LAN/MAN/WAN and Office Automation Systems,
2. Design of multi-vendor LANs interconnected via multiple protocols,
3. Evaluation of LAN/MAN/WAN, and OFFICE AUTOMATION Systems software and hardware,
4. Evaluation, development, planning, installation, operation, maintenance of multi-vendor LAN systems including technologies such as 10/100/1000/10000 Ethernet, Novell, NT, UNIX, TCP/IP, IPX, Corel WordPerfect Office, Novell GroupWise, and the Internet.
5. Any other network related area of expertise as directed by the NRC.

Qualifications:

Education:

Masters level degree from an accredited university or college is required in electrical engineering,

management science, computer science, mathematics, industrial, or other engineering discipline. Fifteen years experience in network technology in general and three years in the requested speciality may be substituted for the educational requirement. Five (5) years experience in network technology and one year in the requested speciality combined with as BS or BA in the delineated fields may be substituted for the educational requirement.

Experience:

At least eight (8) years of technical related experience is desirable, including two (2) years in program/project management. To be effective the individual should have demonstrated analytical and problem solving ability, creativity, and insight in working with networks similar to the NRC's. In addition the individual should have strong verbal and written communication skills.

Special Note:

This position may be a full time position with the Contractor if the NRC agrees that such skills are required on the contract. However, the job description may also be used by the NRC and the Contractor as a method to obtain temporary consulting services in areas of expertise outside that of the Contractor's normal staff.

4.3.7.7 Senior Systems Engineer

POSITION DESCRIPTION

Position: Senior Systems Engineer

Functions: Performs activities associated with the design and implementation of local and wide area networks and office automation systems. Analyzes, designs, integrates documents, implements "state of the art" local and wide area networks, office automation systems and microcomputer systems and applications. Performs comparative analysis of commercial software packages. Conducts scientific and statistical analyses. Conducts user and technical training. Assists LAN Analysts and programmers in the planning, organizing, controlling and scheduling of activities.

Serves as the technical expert in the area of measurement and analysis of LAN, WAN, and OFFICE AUTOMATION systems hardware and software. Measures and reports on the performance of LAN, OFFICE AUTOMATION, ADP, and telecommunications systems. Maintains the performance database, performs performance analysis to identify and seek solutions to performance problems.

Provides administrative and technical consultation on a wide variety of management concerns such as: office and automation studies, system and processing problem areas, areas for potential improvement, and methods and procedures to promote the efficiency and effectiveness of office systems operations. Provides guidance and management analysis capabilities to resolve processing and office system operation problems.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, electronics, mathematics, engineering, statistics, operations research, accounting, business administration, or computer related field is desirable. Ten (10) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

At least eight (8) years experience with progressively more difficult LAN/network responsibility including a minimum of seven (7) years of systems analysis including acting as lead analyst for development of LAN, WAN and OFFICE AUTOMATION systems. This position requires a sound and thorough theoretical and practical knowledge of LAN, WAN and office automation systems. Requires skills in verbal and written communications. It also requires initiative, imagination, analytical ability, and the ability to deal tactfully and effectively with customers and NRC network staff.

4.3.7.8 Systems Consultant

POSITION DESCRIPTION

Title: Systems Consultant

Functions: Major participant in any project or phase of development from problem definition through problem resolution. Works with minimum direct supervision. Responsible for preparing substantial parts of interim and final reports. Can be expected to work on multiple tasks simultaneously and must be able to effectively plan and manage own time. Will have extensive contact with NRC staff as requested by the NRC. Can serve as project manager of small or medium sized projects or portions of larger ones. Will provide expertise in the following areas:

1. Local and Wide Area Networks and office automation Systems,
2. Resource sharing capabilities,
3. Evaluation of LAN, WAN, and office automation systems software and hardware,
4. Development, maintenance, planning, engineering, and management of telecommunications (data communications, communications security, and networking) systems,
5. Development, planning, evaluation and review of LAN, WAN and office automation systems security.
6. Any other network related area of expertise as directed by the NRC.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in management sciences, computer science, mathematics, industrial or other engineering, accounting, or business administration. Ten (10) years experience in network technology in general and one year in the requested speciality may be substituted for the educational requirement.

Experience:

At least 5 years of related experience is required, to include 2 years in professional consulting and 1 year in project management. This position requires proven analytical and problem solving abilities, creativity and insight. Skill in making verbal and written presentations is required.

Special Note:

This position may be a full time position with the Contractor if the NRC agrees that such skills are required on the contract. However, the job description may also be used by the NRC and the Contractor as a method to obtain temporary consulting services in areas of expertise outside that of the Contractor's normal staff

4.3.7.9 UNIX System Analyst

POSITION DESCRIPTION

Position: UNIX System Analyst

Functions: Performs activities associated with the implementation and support of UNIX Systems, and the development and implementation of Local and Wide Area Network services in a UNIX environment. Evaluates, installs, and integrates commercial UNIX software packages. Conducts user and technical training, and provides guidance in the operation of NRC UNIX Workstations and network environments. Provides trouble shooting and problem resolution related to UNIX network environment. Assists LAN Analysts and programmers in the design and development of Novell and UNIX interconnected networks and connectivity. May act as project manager.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, mathematics, engineering statistics, operations, accounting or business administration. Five (5) years directly related experience as a UNIX analyst of which at least two (2) years as a UNIX systems administrator may be substituted for the educational requirement.

Experience:

At least three (3) years experience including two (2) years experience in the UNIX environment. This position requires a sound, thorough, theoretical, and practical knowledge of UNIX, LAN and Office Automation systems. It also requires initiative, imagination, analytical ability, and the ability to deal tactfully and effectively with NRC personnel.

5 PROGRAM SERVICES

Program Services provides continuity and control of specific functions that affect all of the ITID Branches. These function include:

- Quality Management
- Configuration Management
- Contingency Management
- Documentation Management
- Security Management
- Independent Audit and Verification

For each of these functions Program Services has developed a program that is used throughout the ITID Organization by all contractors. Program Services also assists individual Branches and contractors in developing plans, automated systems, metrics, methods for analysis, reporting and other requirements necessary to conform to the program objectives.

5.1 Quality Management

5.1.1 Program Management

- Develop and maintain a Quality Management Program for all services performed.
- Update the plan semi-annually.

5.1.2 Metrics and Performance Criteria

- Assist in developing metrics and performance criteria to determine whether or not established service levels are being met in carrying out their mission.
- Maintain and electronically store performance data derived from automated systems supporting services provided.

5.1.3 End-User Satisfaction Monitoring

- Conduct periodic, statistically significant, random surveys to assess end-user satisfaction with services provided.
- Produce an end-user satisfaction report based on the results of the end-user satisfaction survey.
- Develop and implement procedures to continue to meet service goals.

5.1.4 Trend Analysis

- Develop trend analyses to ensure early identification of areas requiring special attention.
- Perform Trend Analysis as needed.
- Collect Service Request resolution data.
- Monitor hardware problem records for each IT component.
- Monitor software problem records for each IT component.
- Track and report by office, the number of tickets that are simply questions about the use of systems (training requests).
- Recommend changes or solutions to NRC on the following:

    - Problem areas.
    - Information that will assist application training in the NRC Professional Development Center.
    - Changes to the NRC infrastructure that are problematic.
    - Changes in the way development introduces new upgrades to NRC Agency-wide applications, based on how it impacts support and the level of increased effort.
- Monitor and discuss with NRC the observation and record of similar, identical, or repetitive CSC Service Requests, especially those that emanate from one particular office, client, building/floor, or office designation.
- Participate in information gathering or technical problem studies as requested by NRC.

5.1.5 Reporting

- Report monthly on actual performance results as compared to the performance goals.
- Provide weekly and quarterly trend analysis reports.
- Provide CSC Service Request summaries.

5.1.6 OCIO Coordination

- Participate and assist in the integration of services support into all planned upgrades, enhancements, and updates to the NRC infrastructure prior to roll-out.
- Attend meetings to assist in the development and implementation of plans for proposed changes in the operation of applications.

5.1.7 Audits

- Assist in responding to NRC reports generated from independent audits of procedure compliance.

5.2 Configuration Management

5.2.1 Program Management

- Develop and maintain a Configuration Management Program
- Assist in the development of configuration management components specific to other OCIO Groups that will integrate with the ITID Configuration Management Program.

5.2.2 Change Management

- Assist in developing and monitoring procedures for reporting, verifying, and recording all changes made to hardware, software, firmware, and documentation throughout the system's life cycle.

5.2.3 Hardware/Software Inventory

- Develop, implement, and maintain an Inventory Management Program to track the physical equipment within NRC.
    - Assist in developing inventory components specific that will integrate with the ITID Inventory

Management Program.
- Participate in and support the annual inventory of NRC property.
- Provide Property and Supply System (PASS) updates.

5.2.4 Configuration Management Data Base (CMDB)

- Develop and implement a plan for identifying, defining and registering CMDB configuration items.
- Select supporting tools
- Register configuration items.
- Establish the current CMDB baseline.
- Maintain updated information on current systems.

5.2.5 Configuration Reporting

- Provide configuration reports as required.
- Maintain and provide infrastructure maps and logic diagrams as required.

5.3 Contingency Management

5.3.1 Program Management

- Develop and maintain an ITID Contingency Management Program
- Assist in the development of contingency management components specific to other OCIO Groups that will integrate with the ITID Contingency Management Program.

5.3.2 Backup

- Develop and monitor backup policies and procedures to ensure the ability to recover and restore NRC systems, applications, files and data.
- Assist in developing backup schedules for all systems and data.
- Assist in creating back-up copies of system hard drives in compliance with standard operating procedures.
- Assist in validating the integrity of back-up copies.
- Assist in providing for data and system software restoration
- Perform semiannual audits of compliance with backup policies and procedures and report the audit findings to NRC.

5.3.3 Disaster Recovery

- Develop a disaster recovery plan in the event of a catastrophic network failure and/or loss of critical network elements.
- Support a disaster recovery site to ensure viability of recovery at remote sites in the event of NRC headquarters disaster.
- Execute the disaster recovery plan in the event of a catastrophic network failure and/or loss of critical

network elements.

- Assist other OCIO groups in developing individual disaster recovery plans that integrate with the ITID disaster recovery plan.
- Respond identified network disasters as required by the disaster plan and in accordance with NRC policies, procedures and service level requirements.

5.4 Documentation Management

5.4.1 Program Management

- Develop and maintain an ITID Documentation Management Program for use by all services provided to assure the comprehensive, detailed, up-to-date documentation of NRC policies, processes, procedures, systems, applications, and other documentation required for the ongoing maintenance of ITID activities.
- Assist in the development of documentation management components specific to other OCIO Groups that will integrate with the ITID Documentation Management Program.

5.4.2 Procedures

- Develop, document (in a easy-to-access and search manner), and maintain standard operating procedures for all Desktop Systems activities.
- Continually review and comment on Desktop Systems standard operating procedures to improve efficiency, improve user support, reduce cost, or otherwise improve operations of Desktop Systems.
- Provide Standard Operating Procedures to OCIO Project Officer and OCIO staff, as requested.
- Update and modify processes and procedures within 30 days of any significant change.
- Provide assistance implementing OCIO policies and procedures as they pertain to Desktop Systems support issues.
- Respond to NRC independent audits of procedure compliance.

5.5 Security Management

5.5.1 Program Management

- Develop and maintain an ITID Security Management Program for use by all OCIO Groups.
- Be familiar and comply with existing NRC security policies and plans and maintain cognizance of procedures and standards promulgated by the National Institute of Science and Technology (NIST) as well as the commercial environment.
- Assist in the development of security management components specific to other OCIO Groups that will integrate with the ITID Security Management Program.

5.5.2 System

- Identify and develop requirements and implement security measures to ensure appropriate safeguards are in place for all system components and services.
- Assist each OCIO group to:
  - Identify, evaluate, develop, implement and operate automated tools to monitor and manage security.
  - Develop and maintain systems that automatically examine logs for unauthorized access attempts or

suspicious activities.
    - Take necessary action to prevent and stop unauthorized access and/or suspicious activity.
    - Gather and analyze statistical security information and provide recommendations to improve and enhance security.
    - Implement data security, file conversion, and file and data backup policies.
    - Control access to administrator rights and passwords.
    - Ensure all systems have and use security capabilities meeting NRC's minimum standards.
- Provide End-User ID administration.
    - Develop, document, and follow step-by-step account administration processes and procedures for every scenario to assure the continuity of support staff performance.
    - Update the account administration processes and procedures as necessary to conform with current operations.
    - Provide OCIO staff (as identified by the Project Officer) a copy of the account administration processes and procedures.
    - Provide password administration (including resets, automatic expirations).
    - Provide end-user account management.
    - Provide account security precautions.
    - Provide shared file access management and administration.
    - Administer access control lists for directory, library, and categories.
        - Set up system defaults for user and group profiles.
        - Set up default access rights for users and groups.
        - Set up and administer the Administrator group, including adding and deleting users.
    - Maintain user profiles.
        - Support, revise, and implement standards for assignment of privileges.
    - Provide security capabilities for all CSC systems in accordance with NRC policies and procedures.

5.3 Network/Cyber

- Identify and develop requirements and implement security measures to ensure appropriate safeguards are in place for network components, systems and services.
- Identify, evaluate, develop, implement and operate automated tools to monitor and manage network security.
- Develop and maintain systems that automatically examine network access logs for unauthorized access attempts or suspicious activities.
- Take necessary action to prevent and stop unauthorized network access and/or suspicious activity.
- Evaluate, develop, implement and continuously update virus protection software as required for network and desktop components, systems and services.
- Gather and analyze network and desktop statistical security information and provide recommendations to improve and enhance network security.
- Provide recommendations and maintain adequate physical security measures for network components and systems.
- Perform periodic audits to ensure compliance with security procedures and processes and report results to NRC.
- Implement data security, file conversion, and file and data backup policies.
- Provide operational maintenance, upgrade, and support of the NRC Firewall components and systems.

5.5.4 Physical

- Provide recommendations and maintain adequate physical security measures for network components and systems.
- Assist each OCIO group to restrict physical access to rooms with critical systems.
- Assist each OCIO group to control access to facilities where sensitive NRC data may be at risk.

5.5.5 Audits

- Assist each OCIO group to respond to NRC independent audits of compliance with CSC security policies and procedures.

5.6 Independent Audit and Verification

- Perform semiannual audits of compliance with NRC policies and procedures for:
  - Configuration Management
  - Backup
  - Disaster Recovery
  - Documentation
  - Security

- Report the audit findings to NRC.
- Report the findings to other contractors.

6 RELATED NRC IT SERVICES

The following NRC IT services are not covered under this SOW. They are briefly discussed here for formation only.

6.1 TELECOMMUNICATIONS SERVICES

Telecommunications Services provides voice services at the NRC's headquarters location. The NRC participates in GSA's Washington Interagency Telecommunications System (WITS) and FTS2000/FTS2001 programs that provide for local and long distance telephone service to Federal customers in the Washington area.

Telecommunications Services also provide and manage the additional telecommunications contracts that furnish additional services not included in the Governmentwide contracts. The systems and equipment supported include, but are not limited to, CENTREX, ISDN, PBX systems, key systems, facsimiles, pagers, cellular phones, satellite communications, two-way radios, audio and video conferencing systems, and cable TV services. The cable plant operation, support and maintenance is included in this grouping based on budgetary categorization.

Telecommunications Services provide the NRC message center and switchboard, telephone and video conferencing, voice mail, calling cards, pagers, facsimile machines, modems, cellular telephones, wire services, secure communications, telex messages, telecommunications devices for the deaf (TDD), and Emergency Operations Center communications.

2 DATA CENTER SERVICES

The Data Center provides system environments for Agencywide applications, including equipment, administration, operation, and support.

The Data Center provides security, operations, support, and maintenance of all mini and mainframe computer systems.

The following applications are provided through the NRC Data Center and are available for use from any Agencywide desktop system when the appropriate access software is installed. These services are provided 24 hours a day, five days a week, with additional on call support provided as required.

ADAMS	Voter Tracking System
Payroll	Commissioner's Calendar
Personnel	EXSIS
Property	GLDB
Criminal History	SIMS
Thesaurus	LMS
STARFIRE	Emergency Response Data System (ERDS)
	Allegation Management System (AMS)
	Executive Shared Information System (EXSIS)

The following applications are provided through a timesharing service. The applications are available from

Agencywide desktop systems when special Agencywide software is installed and a valid user account is issued.

Regulatory Information Tracking System
Agency Training System
Automated Personnel System
Annual Material License Fee
Operator Licensing Tracking System
Manpower System
Technical Assignment Control System

The following applications will be provided through a timesharing service until STARFIRE (the NRC administration services program) is fully implemented and supported.

Federal Financial Management System (FMS) (120 accounts)
NRC's Financial and Accounting Applications (120 accounts)
Payroll/Personnel System (1,076 accounts)
Production Time and Attendance Data Entry (1,076)

6.3 EMERGENCY OPERATIONS CENTER

OCIO provides operation and maintenance support to the IT Infrastructure components located in the NRC Emergency Operations Center on the 6th floor of Two White Flint North. Some SMS support will be required each time the Center is fully activated.

NRC's Emergency Operations Center is intended to ensure the continued, uninterrupted exchange of information between HQ and any incident site involving nuclear materials, including the four Regional Offices, Nuclear Power Plans, fuel and waste sites, and other governmental agencies.

Within the Washington, D.C. metropolitan area, NRC uses Verizon, FTS 2001, GSA Consolidated Local Services, and WITS, as well as sharing services with the Department of the Interiors National Interagency Fire Center.

In addition to the refresh, maintenance and support of desktops, servers and peripherals, ITID is responsible for performing the following tasks for the Emergency Operations Center:

1) Provide the facilities, services, and equipment required to support both wire, and wireless voice, data and video communications.
2) Provide Emergency Telecommunications Specialist Coordination support.
3) Update and distribute current copies of the PBX system charts.
4) Maintain the Emergency Telecommunications Response Workbook.
5) Provide operation and maintenance of the PBX system and associated telecom equipment and services.

UNITED STATES NUCLEAR REGULATORY COMMISSION

Office of the
Chief Information Officer
Information Technology Infrastructure Division

Information Technology Architecture

Version 1.0

September 13, 1999

Introduction

Purpose

This document describes the United States Nuclear Regulatory Commission's Information Technology Architecture (ITA) as required by the Clinger-Cohen Act of 1996 (Public Law 104-106) and Office of Management and Budget Memorandum M-97-16.

Background

The Clinger-Cohen Act assigns the Chief Information Officer (CIO) the responsibility of "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture."

The Clinger-Cohen Act defines the ITA as:

> *... an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals. (Section 5125 (d))*

The Office of Management and Budget, in its Memorandum M-97-16 on the subject of "Information Technology Architectures" states:

> The ITA is broad in scope and includes processes and products. An architecture in compliance with the Clinger-Cohen Act and OMB guidance will contain two elements :
>
> - the Enterprise Architecture,
> - a Technical Reference Model and Standards Profiles.

Enterprise Architecture

The Enterprise Architecture at the NRC is described in this document. The architecture consists of the topology and technical standards used throughout the agency to support the major systems and networks.

Technical Reference Model and Standards Profiles

The Technical Reference Model at the NRC is a separate document, published periodically, that describes the legacy, preferred, and target standards in each of several functional areas for the NRC's desktop, server, and mini/mainframe computer systems. It also identifies the "to be avoided" technologies for the agency. It supports the objectives of the Enterprise Architecture at the tactical level by identifying specific protocols, standards and commercial products acceptable to the agency to implement the Enterprise Architecture.

Overview of the NRC's Information Technology Architecture

The NRC's Information Technology (IT) Architecture is designed to provide a standard method for delivering IT services to the desktop of employees and designated contractors, as well as facilitate communications with external organizations such as other domestic and foreign government agencies, nuclear power plants, and other clients, laboratories and the general public. The agency's computer centers include servers and mini-computers. These are connected to the Rockville headquarters backbone network. Other networks, Internet services, and timesharing services are also connected through Rockville after passing through a firewall. The NRC's Enterprise Network Architecture is shown in Figure 1.

All agency personnel are provided with a standard desktop workstation that is an Intel-based processor using the Microsoft NT Workstation operating system. The workstation is connected to an Ethernet local area network (LAN). Each NRC location uses the same architecture for its LAN installations. This standardization makes operations and maintenance consistent throughout the agency, and eases the implementation of new agencywide applications and services.

The LANs are all connected to the headquarters backbone network. The NRC's other IT systems and services are also connected to the NRC backbone network, through a series of inter-connected hubs, routers, and switches. The regional wide area network and backbone connections use Asynchronous Transfer Mode (ATM) to maintain maximum speed, inter-operability, and security as well as provide the potential for any-to-any communications. Internet Engineering Task Force's (IETF) Internet Protocol (IP) and Novell's Internet Package Exchange (IPX) protocol are used in the network. IPX will be phased out as Novell provides full support for IP protocol.

In addition to its internal private network, the NRC uses services from various external sources, such as Internet services and other government agency timesharing services. The NRC coordinates with these services to install connections that would make the service accessible to the NRC users via the standard desktop workstation systems. The preferred mode of access is through the existing LAN infrastructure using standard remote LAN protocols or ATM.

The remainder of this document discusses the architecture in more detail and is organized as follows:

- Wide Area Network (WAN) Architecture
- Local Area Network (LAN) Architecture
- Computer Center Architecture
- Three-Tiered Architecture Protocols

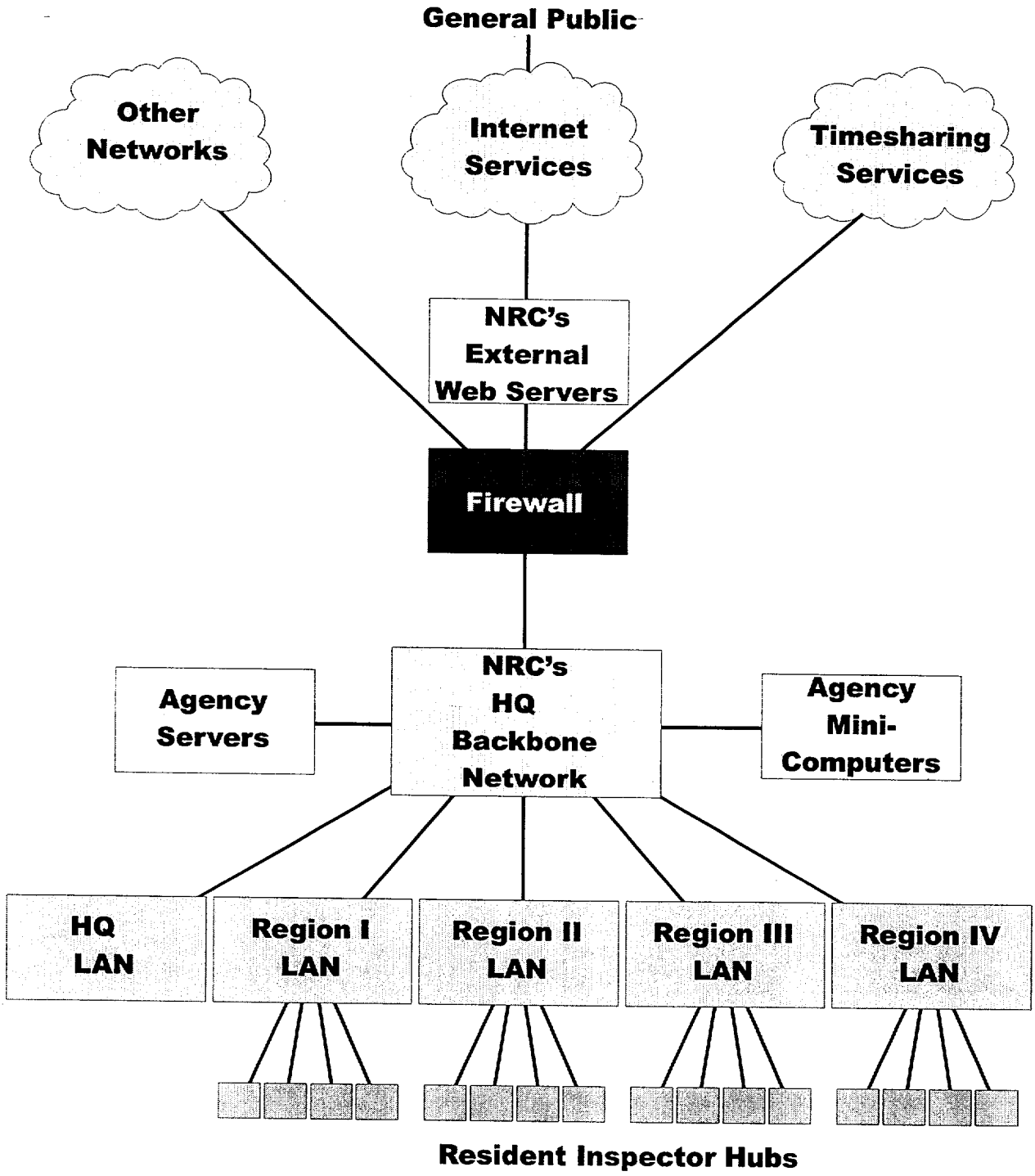


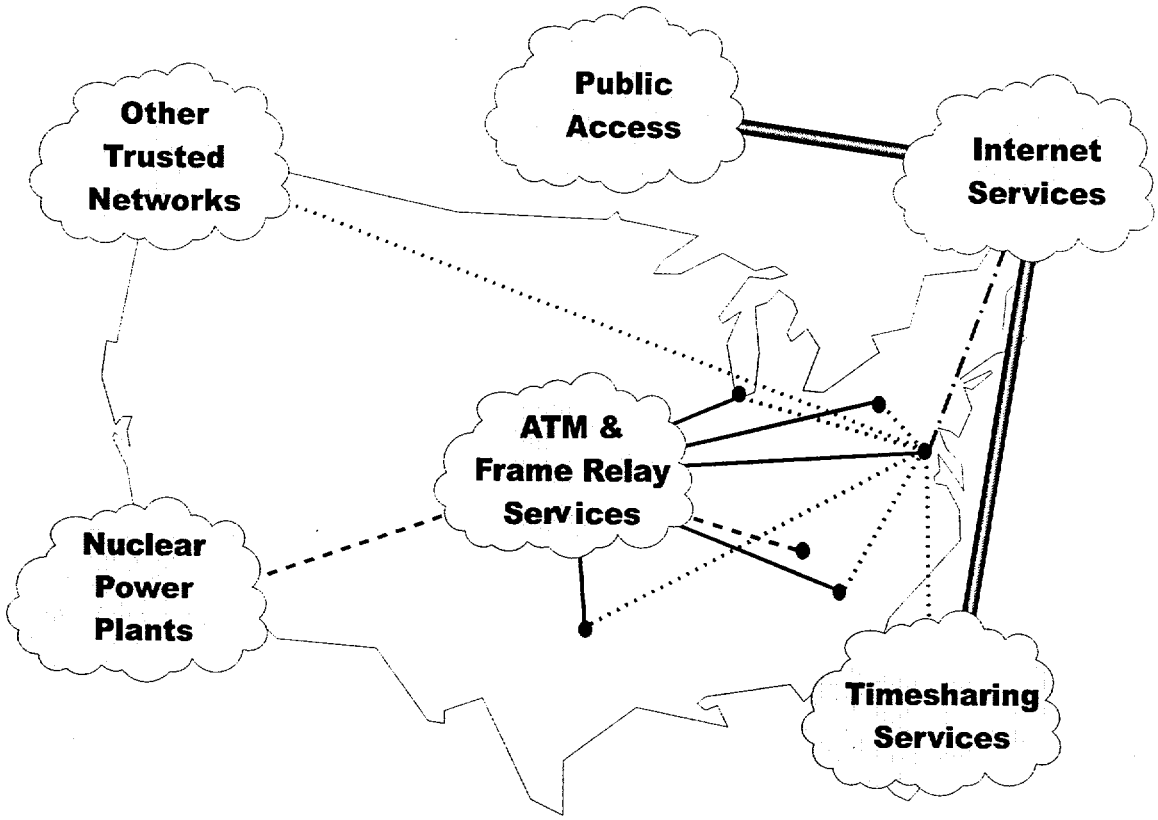
Figure 1. NRC's Enterprise Network Architecture.

NRC Wide Area Network (WAN) Technologies

The agency's Wide Area Network architecture calls for higher speed communications to connect the headquarters backbone network to other NRC locations in the Washington area, contractor locations, NRC regional offices, the nuclear power plant sites, timesharing service providers, and Internet service providers. Other networks are connected with a combination of high and low speed services, depending on the capacity and response time requirements. The NRC requires that all WAN services be terminated with equipment that will support Internet Engineering Task Force (IETF) Transmission Control Protocol (TCP) over Internet Protocol (IP).

The NRC's high speed services outside of the Rockville metropolitan area are switched digital WAN protocols. Figure 2 shows the geographic locations served by the NRC enterprise WAN. The NRC's headquarters, in Rockville, Maryland, is the central point of the architecture with Asynchronous Transfer Mode (ATM) connections to all of the regional offices. Frame relay services connect the nuclear power plants to the regional offices. Frame relay is also used to connect the agency's training center to the Rockville backbone. The logical layer protocol is ATM Adaptation Layer (AAL) between headquarters and the regions and IEEE 802.3 (CSMA/CD Media Access Control - Ethernet 10 Base-T) between the regions and the nuclear power plant sites. A legacy T-1 network is used for video teleconferencing between headquarters and the regional offices.

In the Rockville area, because of the availability of fiber-based technologies, the NRC is using Bell Atlantic's Fiber Distributed Data Interface (FDDI) Network Services (FNS) for local high capacity connections to the agency's Internet service provider and its IT support contractor. The logical layer protocols supported by this service are IEEE 802.3 (Ethernet) and IEEE 802.5 (Token Ring). A variety of other services are also employed for local connections to other networks, including full T-1/DS-1, fractional T-1, dedicated digital services, and dial-up services.



ATM
Frame Relay
Fiber Distributed Data Interface (FDDI) Network Services (FNS)
Dedicated Digital Services (DDS), Fractional or Full T-1/DS-1
Various Technologies

Figure 2. NRC Wide Area Network Technologies.

Local Area Network (LAN) Architecture

The NRC connects all of its Intel-based processor desktop workstations to a Local Area Network (LAN) hub. Other types of connections are discouraged and every effort is made to accommodate various access requirements within the LAN architecture. Figure 3 shows the architecture for a typical building at the agency.

Up to 160 desktop workstations, printers, office servers, or other Ethernet capable devices can be connected to a single LAN hub. The agency uses at least one switched Ethernet 10Base-T hub on each floor in a building. These are connected, via multi-mode fiber, to central backbone switching hubs located in a computer center in the building. The protocol for hub-to-hub communications is ATM. There are at least two backbone hubs per building. All hubs are fully redundant, with dual processors and dual backplane capability. The hubs that serve the individual floors are connected to at least two backbone switching hubs for further redundancy. The backbone switching hubs are used to interconnect the buildings and remote locations.

At the regional offices, the architecture of the LANs is essentially the same. Identical ATM/Ethernet switching hubs are used in all locations. The regional offices and headquarters are interconnected via one set of backbone hubs at each location that is configured for ATM communications over the WAN.

The regional offices are connected into the Nuclear Plant Sites using smaller shared Ethernet hubs with remote communications capability to connect to the regional backbone hubs. Frame relay connections accommodate these locations.

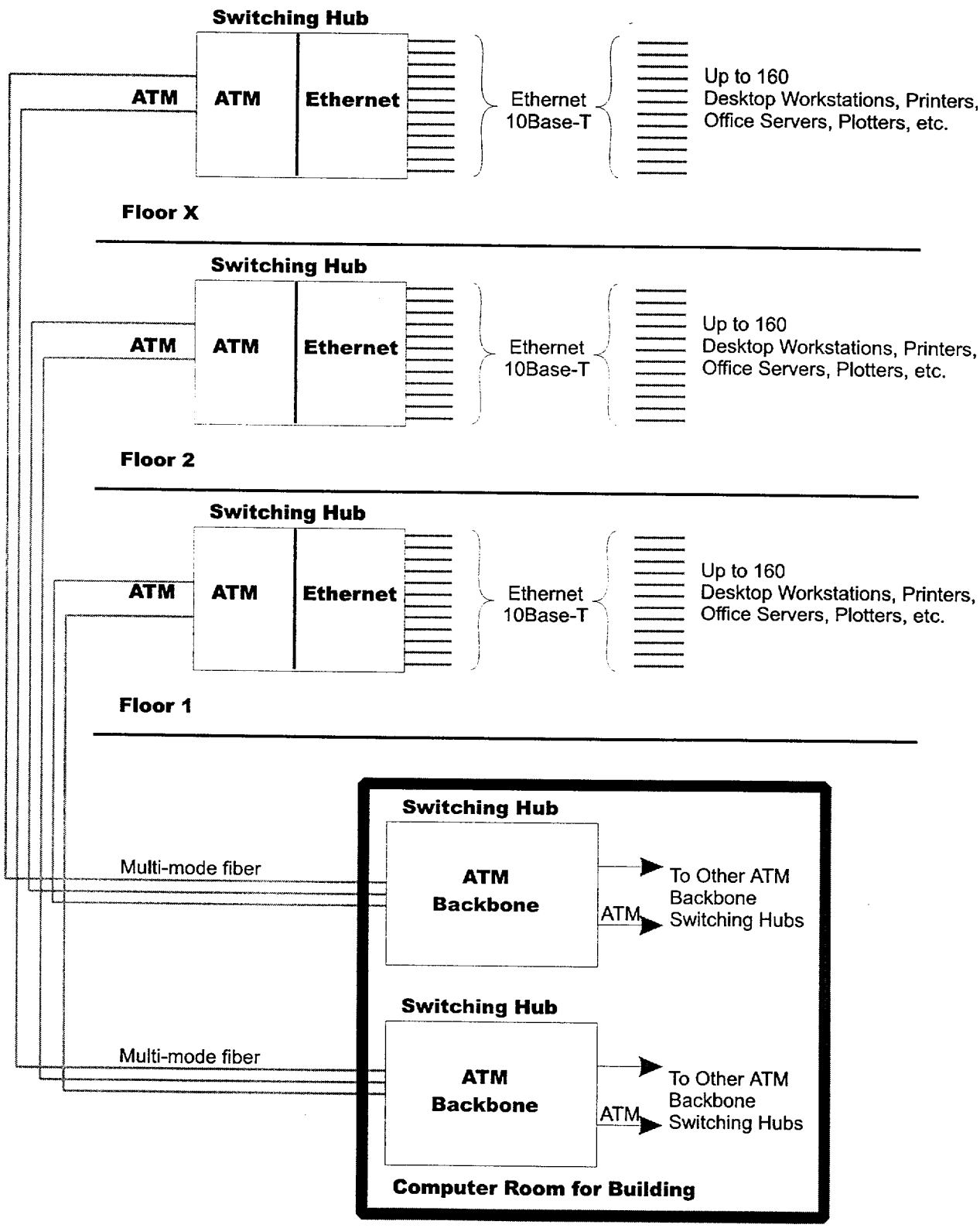


Figure 3. NRC's Local Area Network (LAN) Architecture.

Computer Center Architecture

The NRC is migrating toward a three-tiered architecture that includes desktop processors and office servers at the first tier, agencywide servers at the second tier, and mini-computers, mainframes, and external services in the third tier.

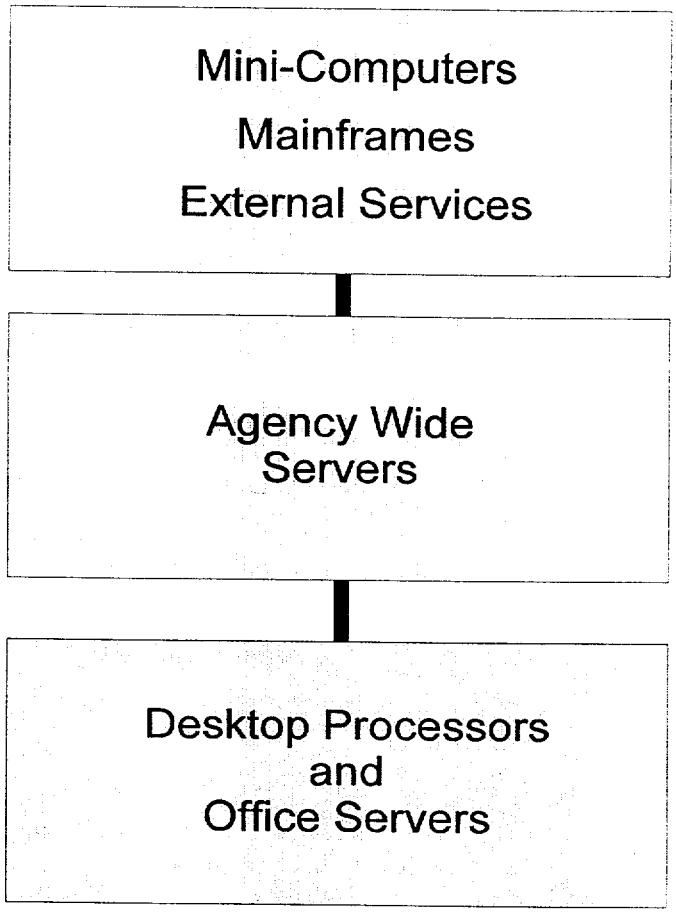


Figure 4. Three-tiered Application System Architecture

First Tier. Desktop processors and office servers are located in the office areas and connected through 10MB switched Ethernet connections. Print servers are also located in the office areas. The agency infrastructure support organization maintains most of the devices in the first tier, including the desktop systems, print servers, and printers that are LAN connected, and some specialized high performance computers. Other devices may be connected to the agency-wide

network or the local LAN as first-tier devices provided they meet minimum requirements for connection and do not disrupt operations of other systems.

Second Tier. The second tier contains most of the agency's server systems. The NRC has centralized its E-mail, network, and agency-wide application servers into computer rooms in each building. The servers are directly connected to the ATM backbone switching hubs shown in Figure 3 with ATM Network Interface Cards (NICs) and multi-mode fiber connections. This architecture provides backbone network speeds for connecting the servers to any floor on the LAN in the local campus. It reduces the reliance on user proximity for client/server application network performance. Servers no longer have to be located on the same floor as the clients that they serve. Availability of the servers can be centrally monitored and managed by the hub systems as well as by an independent centralized network management system. The load on each server can be monitored and balanced with other servers as necessary. The ability to observe and access the server systems from a single location provides more efficient use of support personnel and more effective and timely operational and maintenance support.

In addition to being centrally located, the NRC servers have been divided into functional groupings. This facilitates the planning for standard systems and interfaces. Different functional groups of servers may require different standard hardware and software configurations and architectural interfaces in order to effectively perform their function. The functional groupings are as follows:

Second Tier Agencywide Servers

Server Category	File Servers	Messaging Servers	Print Servers	Applications Servers	Database Servers	Gateway Servers
Function	File and Mass Data Storage Services	Messaging and E-Mail Services	Print Queue Storage Buffers Shared Printer Network Connectivity	Specialized Client/Server Application Processing	Client/Server Database Services	Gates Between Unlike Networks or Operating System Environments

For additional information on the configurations and operating environments for servers, refer to the Technical Reference Model dated January 4, 1999.

Third Tier. The third tier in the NRC Application System Architecture consists of legacy mainframe and mini-computer systems, and other connections to external networks and services. There are a wide variety of configurations and interfaces necessary for connections and inter-operability with these systems. At the core of the NRC's third tier architecture is the assumption that standard protocols will be used wherever possible and the Internet Engineering Task Force (IETF) protocols will be supported and encouraged to the greatest extent possible.

Three-Tiered Architecture Protocols

Physical and Logical Layer. The physical and logical layer protocols for the first tier is switched Ethernet 10Base-T. For the second tier, the protocol is ATM. For the third tier, the NRC has a number of different physical and logical layer protocols that have been implemented to accommodate external networks. All are translated to ATM for routing through the NRC backbone, then to the standard IEEE 10Base-T and IEEE 802.3 (Ethernet) for delivery to the desktop. Although the transport system of choice for client/server communications is Internet Protocol (IP), there are some legacy systems running Novell IPX. These will be retired with the implementation of Novell's full IP support in FY 2000.

Network Layer. The NRC has put considerable emphasis on the standardization of network protocols in the three tiers of its architecture in order to provide a network infrastructure that provides maximum inter-operability between systems. The standard method for employees to access third tier external networks and services is through their first tier desktop systems. Third tier systems must traverse the first and second tier systems in order reach their target clients on the first tier desktop systems. Internet Protocol (IP) has been implemented as the standard network layer interface to these external sources. It can be supported in all three tiers and it can support the packet delivery services of Transmission Control Protocol (TCP) at the transport layer.

Transport, Session and Application Layers. The NRC uses a variety of methods for external applications to address client software on desktop systems, establish sessions, and establish application to application communications. Although the vision of the agency is to find a single method for inter-operability with external applications, the agreement on commercial open system technologies required to implement this is still far in the future. In the meantime, the NRC is using some of the more widely accepted methods, such as the IETF defined service technologies: Transmission Control Protocol (TCP), HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), TELNET Virtual Terminal, and Simple Mail Transfer Protocol (SMTP). The NRC also supports Secure Sockets Layer (SSL).

Summary. The primary protocols supported in the three-tiered architecture are shown in Figure 5.

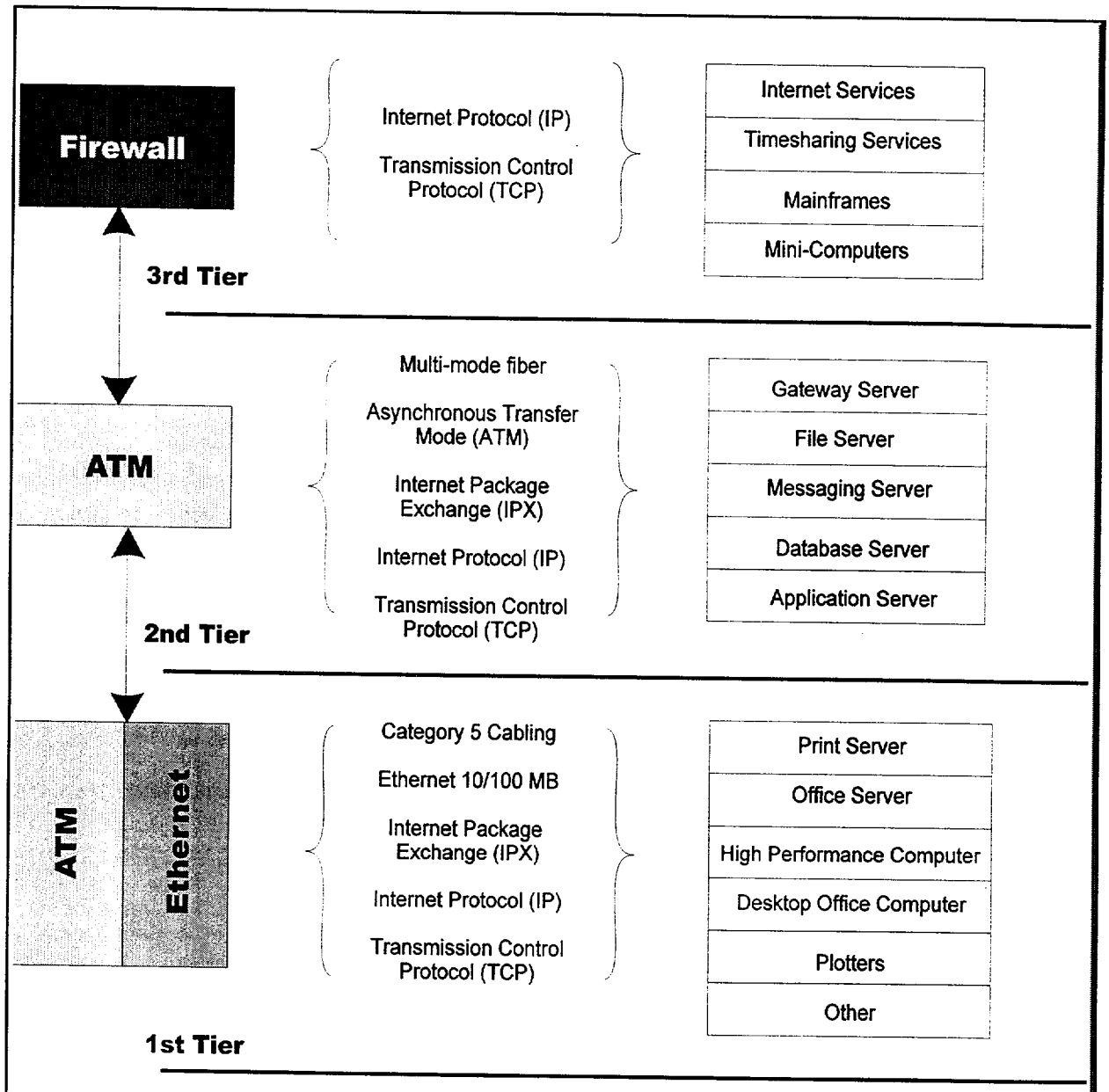


Figure 5. Three-Tiered Architecture Protocols

Infrastructure Development Process Model

Version 1.1

January 31, 2000

Infrastructure Development Process Model

Table of Contents

1.0 Background 1

2.0 Purpose 1

3.0 Approach 1

4.0 Overview of the IDPM 2

5.0 Overview of the Ten Phases 3
- 5.1 Detailed Requirements Analysis 4
- 5.2 Detailed Design 5
- 5.3 New Technology Development 6
- 5.4 New Technology Acceptance Testing 7
- 5.5 Integration Into the POE 8
- 5.6 Operational Acceptance Testing 9
- 5.7 Transition to Support 10
- 5.8 Implementation and Training 11
- 5.9 Operation and Support 11
- 5.10 Decommissioning and Disposal 12

Attachment A - Generic Primavera Schedules for all Ten Phases A-1

List of Figures

Figure 1 Ten Phases of the IDPM 2

1.0 Background

Sytel, Inc. of Bethesda, MD is the successful offeror on the U.S. Nuclear Regulatory Commission's (NRC), "Next Generation Network" contract. With its subcontractor, CEXEC, Inc., Sytel will be supporting the NRC's existing Agency Wide Network (AWN), while designing, developing, and installing the Agency's Next Generation Network (NGN).

2.0 Purpose

This document outlines the Integrated Development Process Model (IDPM), describing the optimal method for adding new technology to the Production Operations Environment (POE), or modifying existing systems, while maintaining the stability and reliability of the POE. The IDPM is a series of standardized repeatable processes that will provide many benefits. Following the IDPM also ensures that the effectiveness of the new technology will be maximized, and that support costs will remain low. The IDPM forms the framework around which all additions, deletions, and changes to the Production Operations Environment (POE) will be accomplished. The IDPM will define all of the phases required to take an integration project through its full life cycle.

3.0 Approach

This document is an overview of the ten phases of the IDPM, explaining the general steps and purposes of each phase. Additional documents are being developed which describe each phase in detail, and provide examples. The IDPM covers the implementation of all types of new technology and the modification of existing systems. For practical purposes, there are three types of new technology: software, hardware, and systems which are comprised of both software and hardware. Where necessary, this document will distinguish among the types of new technology being deployed.

In the planning of the implementation of a new technology, or a modification to existing systems, all ten phases should be included. However, only some of the steps within each phase will be appropriate for a given implementation, requirement, or modification. This will be most notable in the case of a modification. Key factors in determining which steps should be emphasized, and which steps excluded include:

- Whether the new system is an upgrade, or the introduction of a new application or technology to the POE;
- Whether the new technology being implemented is software, hardware, or a system;
- Whether, and to what degree, the new technology, or modification will change the way users work, or interrupt their work during implementation;
- The number and type of NRC offices affected by the new technology or modification;
- The size of the new system; and
- The age and condition of the existing system in the case of a modification.

These issues will be addressed further in the detail documents about each of the ten phases. Section 4 of this document will provide an overview of the whole model. Section 5 will give a brief introduction to each of the ten phases. Attachment A is a generic schedule created in Primavera Project and includes the major steps of the ten phases and their dependencies.

4.0 Overview of the IDPM

The Integrated Development Process Model is a customization of a standard Information Technology System Development Life Cycle (SDLC) to best meet the needs of the NRC POE. The goal is to follow a standard method of developing and deploying all applications and systems which add to or change the POE so that the POE and the new technology can remain stable and be supported. The IDPM also integrates the lessons learned from past successes and difficulties in development, testing, implementation and support. The ten phases of the IDPM ensure sufficient attention to key aspects of the process. For simplicity, wherever new technology is referenced, it will be inclusive of any new additions to the POE as well as modifications to existing POE systems.

To put it simply, any new technology developed and implemented carefully according to the IDPM will be reliable on the NRC network and valuable to the people who use it. Additionally, modifications made to existing systems will not disrupt current capabilities of the affected systems, but will enhance them or they will not be implemented.

Figure 1 illustrates the ten phases of the IDPM, in order. Each phase must be completed before the next phase can begin. For example, Phase 4, New Technology Acceptance Testing, includes the possibility that the new technology will be found to be unworkable in its current version, and will be sent back for redesign. Therefore, Phase 5, Integration into the POE, should never begin until Phase 4, New Technology Acceptance Testing, is complete.

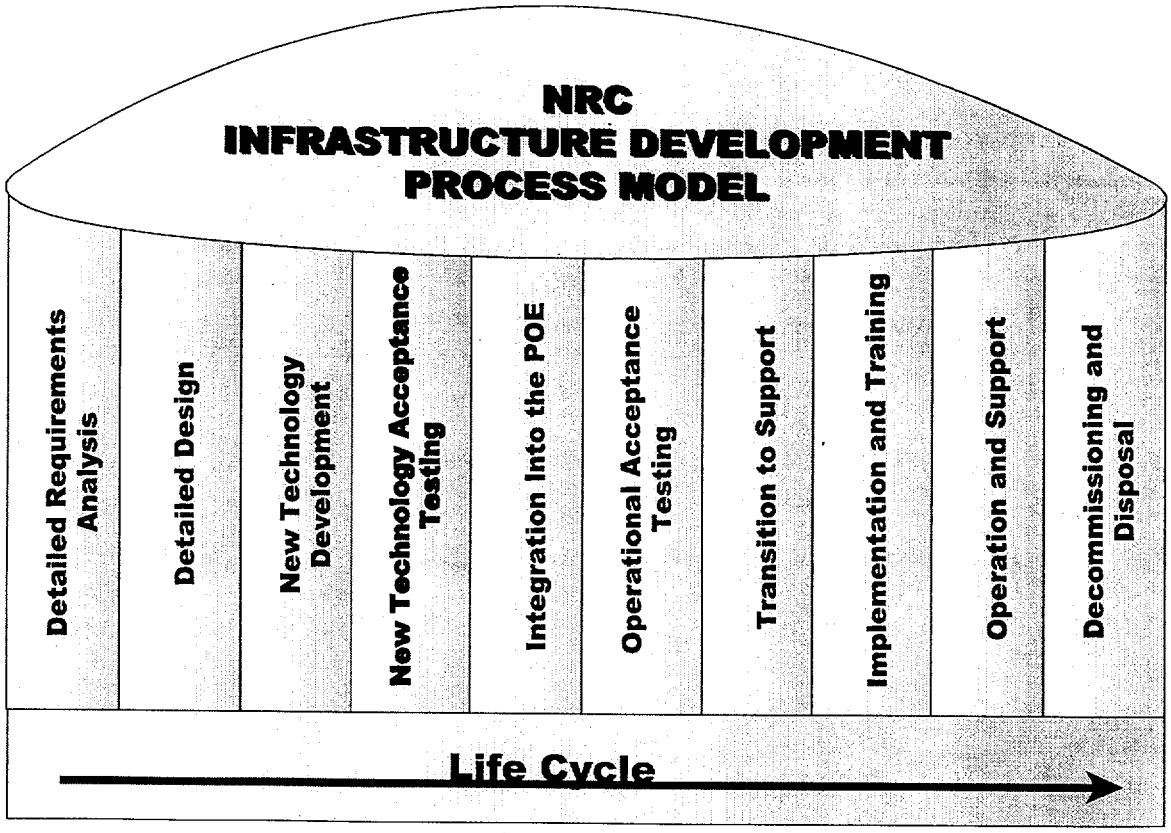


Figure 1 Ten Phases of the IDPM

There is one very important note to make regarding testing. All of the phases include some review and/or testing steps. Passing a review or test is not automatic for a new technology. In an ideal project, the tests would be run, the product would pass, and the next steps, or next phase, would begin. In reality, this never happens. Tests find problems that require minor repair, documentation revision, or major rework. Then the tests must be run again. Only when the test is passed can the project move on to the next steps or phases.

Testing, therefore, brings an iterative component into the life cycle. The technical details of tests and handling of test failures are left to the detail documents. However, at this level, three elements must be recognized:

- It is not appropriate to push development of a new technology forward when it does not pass the tests. Usability and reliability must be proven before the next step of development or deployment begins. Otherwise, time and cost will both spiral out of control, and lower quality will create reliability problems for the new technology, and possibly for the entire POE.

- Since it is impossible to predict what failures will occur during testing, it is impossible to predict how long a testing/repair cycle will take. The IDPM includes the best available methods for making estimates, but actual schedules will vary. If the overall IDPM schedule is created properly, and it is followed carefully with appropriate resources assigned to each step, then the new technology will be ready for deployment on schedule.

- Testing is crucial. Errors in any one phase, if passed onto the subsequent phase, generally cost ten times as much to fix in the next phase as they would have cost in the phase in which they occurred and that cost will increase logarithmically for each subsequent phase in which they remain unfixed.

5.0 Entry Point and Description of the Ten Phases

Each of the ten phases is described here. The description includes the purpose of the phase, the prior work that must be completed so that the phase can begin, the goal of the phase, and the steps of the phase.

In most cases, this document does not define who will do the work of each phase. The organization (NRC division, vendor, or consulting group) who will perform the work varies depending on the type and size of the project. The detail documents will provide an explanation of which group will do a phase for a particular kind of new technology that is being developed. However, in cases where a phase is always performed by a given group, the group is identified in this document.

The purpose of the phase explains the core value of the work entailed in the phase. The prior work that must be completed (usually completion of the prior phase) describes what must have already been done so that the phase can begin. The goal of the phase describes the concrete deliverables–usually items ready for testing, or tested, approved items ready for the next phase. The steps are the task items that comprise the phase. The deliverable into Phase 1 will be a Task Requirements Outline that has been approved by the Operations Configuration Control Board (OCCB) as something that should be developed and deployed into the POE.

5.1 Detailed Requirements Analysis

The purpose of the detailed requirements analysis is for the users of the new technology to define what the new technology must do to enhance the way they work, defining the purpose of the new technology. The need for change arises with the end user, either because new work is being performed, or because the existing system is not providing what is needed for work to be done effectively or efficiently. Only the user (or supervisor of a group of users) can describe what it is they need the system to do.

If the purpose of the new technology is carefully created and verified in this phase, then the final product will suit the user's needs. If the purpose is not defined clearly enough, the product will not improve the work of the people who use it. Precision in the determination and documentation for the requirement is critical at this phase. It is possible that there is an existing system that can provide their required functionality that the users are unaware of. It is also possible that there is an existing system that can be modified to provide the required functionality.

The first key to success in any project is a thorough understanding of the goals. Without well defined user requirements, those goals cannot be set and therefore will never be reached. Industry analysis clearly points to lack of requirements or shifting requirements as a major cause of information technology (IT) integration failures.

The second key to success is a thorough understanding of what the users will be doing with the new technology. Processes must be well documented and understood before any design work can take place. It is even very possible that a new technology is not required, just a re-engineering of the existing processes. It is a common myth that technology can solve problems in processes. This of course is not true and will only lead to a more efficiently executed bad process. Interview and process documentation performed by systems analysts are required before any detailed requirements or design documents can be written. Again, research shows poor analysis to be another major cause of IT integration failure.

The detailed requirements analysis is the first phase of the IDPM, so nothing needs to be done before it begins.

The goal of the detailed requirements analysis is a document that accurately describes needs that the new technology will fulfill and the environment into which the new technology will be placed.

The steps of the detailed requirements analysis are:

1. Meetings between NRC users and technical staff to define the users' requirements;
2. Analysis of processes affected, created, or eliminated by the new technology;
3. Identification of other users who will use or be affected by the new technology, and inclusion of their needs;
4. Identification of any specialized, labor intensive or unusual support requirements needed by the users;
5. A conceptual review of the parts of the POE that the new technology will interact with;
6. A determination of feasibility (if the project is not found to be feasible, it is canceled before resources are spent on design);

7. Production of an analysis document, form the Task Requirements Outline, which provides:
   A. The project name;
   B. A description of the scope of the project, including which divisions of the NRC will and will not use the new technology, and what the new technology will and will not do;
   C. The primary users' detailed needs requirements;
   D. Secondary users' detailed needs requirements;
   E. A list of all parts of the POE which are affected by this new technology;
   F. A description of the parts of the POE which interact closely with the new technology, requiring the greatest design and testing efforts; and
   G. An initial draft project budget and schedule.
8. Approval of this detailed requirements analysis document by all stake holders;
9. Approval of funding for the design phase. If there is a commitment to proceed with the entire project, approval of funding for the entire project;

RM/CM

10. The Requirements analysis document is sent to the OCCB for approval;
11. If Approved, the Requirements Analysis is sent to Release Management to assign Release Candidate status and target release dates.

5.2 Detailed Design

The purpose of the detailed design phase is to design the new system and the project which will create it. A proper conceptual design, technical design, and project plan ensure that the project can move ahead to deliver a new technology that will be useful when it is implemented.

Before the detailed design phase can begin, the detailed requirements analysis must be completed and approved by all parties. In addition, funding for the design, or for the whole project, must be approved.

The goals of the design phase are:

- A completed detailed conceptual design;
- A completed technical design;
- A project schedule;
- A budget covering all remaining phases of the IDPM for this project;
- Design of monitoring and maintenance tools for the new technology through integration into the Integrated Network Monitoring System (INMS); and
- An upper level outline for the support, operations, and maintenance of the new technology.

The steps of the detailed design phase are:

1. Identification of the technical teams involved in design and development;
2. Creation of detailed functional specifications;
3. Preparation of a detailed conceptual design;
4. Determination of the type of project: new software, new hardware, new multi-component system, or modifications to existing systems;

5. Determination of the size of the project: small (such as an upgrade), or large (such as a new system implementation);
6. Determination of whether the new technology will be purchased as is, purchased and customized, or created as a custom application or system;
7. Approval of the functional specifications and conceptual design by the technical groups that will be involved in the project;
8. Preparation of one or more technical designs, with product specifications, time and budget estimates;
9. If more than one technical design is prepared, a preparation comparison chart to help the requestor's technical representative determine which is the best choice, and, if appropriate, a recommendation of one of the alternatives;
10. A technical review of the parts of the POE that the new technology will interact with;
11. An integration plan that focuses on the interactions between the services and interfaces available as part of the POE and the requirements of the new technology for interfaces and services to operate correctly and communicate on all levels with end users and existing POE systems;
12. A go/no go decision on the entire project, if this was not done in Phase 1;
13. A selection among the technical design options approved by the requestor's technical representative, any appropriate applications acquisition or development team, ITID/IDIB, ITID/IOB, and ITID/CSB;
14. Budget approval for the remaining eight phases of the project, if this has not already been obtained in Phase 1.

5.3 New Technology Development

The purpose of the new technology development phase is the actual creation of the new software, hardware, or multi-component system which will be used at the NRC. The product may be acquired (as in the purchase of COTS software, such as the Corel 8 suite), assembled and customized (as in the development of a system built of multiple hardware and software components, and then customized, such as ADAMS or Citrix Remote Access), or developed as custom software.

Before the new technology development phase can begin, the detailed design phase must be completed, with the conceptual and technical design approved, a functional specification approved, the departments involved identified, and funding approved and assigned.

The goals of the new technology development phase are:

- A working application, hardware component, or multi-component system ready for testing;
- Development of monitoring and maintenance tools for the new technology through integration into the Integrated Network Monitoring System (INMS); and
- A support, operations, and maintenance plan for the new technology.

The steps of the new technology development phase are:

1. Review of the technical design;
2. Determination of the roles of all stake holders staff, including the Project Requestor, the contacts for other affected divisions, and the project owner;

3. Selection of vendors and consultants, either per current contract, through subcontracting, selection, or a bidding process, as determined by policy and legal requirements;
4. Purchase and/or build the components;
5. Assemble and/or build the system;
6. Custom integration as required;
7. Changes to the technical design, as needed;
8. Development of the tools needed to be added or modified in the INMS to provide automated monitoring of the new technology and to provide the data required for reporting;
9. Preparation of a user guide and any changes required of the detailed design document and technical specifications and if so, reapproval of the new documents;
10. Preparation of the support, operations and maintenance plan for the new technology;
11. Preparation and approval of a comprehensive test plan based on the functional specifications;
12. Internal testing, in an isolated controlled environment, by the development group to help assure that the product can pass the formal acceptance tests in the next phase.

5.4 New Technology Acceptance Testing

The purpose of the new technology acceptance testing phase is to assure that the new technology works, providing users with the functionality determined in the Requirements Analysis, and also working in the technology environment of the POE.

Before the new technology acceptance testing phase can begin, the new technology development phase must be completed. **NOTE:** The initial scheduling steps (below) begin once the new technology development phase is completed, and the developers know when they will be able to deliver a working system.

The goal of the new technology acceptance testing phase is a working system that is approved and ready for the development work necessary to integrate it into the POE.

The steps of the new technology acceptance testing phase are:

1. The group performing the new technology development informs the stake holders of a delivery date when the new technology will be delivered for testing;
2. A test group is formed that will perform the tests in accordance with the acceptance test plan;
3. The stake holders review the Acceptance Test Plan and determine who (the NRC, an independent consultant, etc.) will perform the acceptance tests;
4. The acceptance test platform is set up. This is not a pilot test, so the application is not tested in the live POE. An isolated test facility will be used that mimics the current POE;
5. If desirable, users willing to participate in the tests along with the testers are found, and the tests are scheduled;
6. The testers set up the test environment and install the new technology. This is part of the test. Installation failures indicate problems with the new technology under development;
7. The user tests are performed to assure that the application will meet the needs of NRC staff per the original analysis;
8. Testing of the INMS monitoring and support of the new technology;

9. Load and stress, functionality, and other tests as defined in the Acceptance Test Plan, are performed;
10. If any minor problems are found, they are resolved by the developers from the new technology development team and the tests are run again, as many times as needed until the deficiencies are corrected;
11. If any major problems are found, the new technology is returned to Phase 4, new technology development for rework;
12. If any changes are made, all test series are re-run. Version control is in place at all times;
13. All test results are documented and published;

CM/RM

14. Configuration Management and Release Management review test results and documentation done to this point;
15. Any adjustments to the Release Schedule are made;
16. Once the new technology has passed all tests, it is approved to proceed by the OCCB.

5.5 Integration Into the POE

The purpose of the integration into the POE phase is to resolve all problems between the new technology and the POE to make sure that the new technology is reliable on the POE and will have the lowest possible support cost. This integration phase involves taking the newly developed technology that has been tested as a unit and "fitting" it into the POE to ensure that all interfaces and services that the new technology requires or uses are available and compatible with the standard interfaces and services provided by the POE. Invariably any integration effort will uncover reliability and compatibility issues that were not discovered in the new technology acceptance testing phase. These need to be resolved prior to the operational acceptance testing phase and should become elements in the test plan, if they are severe enough, so that it can be confirmed that any integration issues arising at this phase are indeed corrected. As is the purpose with an integration effort, there may arise requirements for additional components to be added to the new technology, or the modification of existing components to provide physical, data and semantic compatibility with the POE. These components should be incorporated into all design, development and test documentation prior to the operational acceptance testing phase.

Before the integration into the POE phase can begin the new technology acceptance testing phase must be completed.

The goals of the integration into the POE phase are:

- Resolution of all reliability and compatibility issues that arise during the integration effort, so that the product is functional, and the product and the POE are reliable when working together;
- Creation and testing of a deployment method;
- Completion of an operational acceptance test plan, an integration design document, an implementation plan, and a support plan;
- Final testing, editing and preparation of user guides and other end-user documentation;

- Implementation of the monitoring and maintenance tools for the new technology through integration into the Integrated Network Monitoring System (INMS); and
- Validation of the support, operations, and maintenance plan for the new technology.

The steps of the integration into the POE phase are:

1. Update project schedule based on estimates from the master schedule and including any adjustments that may be required so that a new technology has actually been developed and tested;
2. Determination of optimal deployment methods;
3. Resolution of all remaining compatibility and reliability issues;
4. Identification and resolution of issues of alternative deployment methods to remote locations;
5. Validation of a support, operations and maintenance plan, and all of the tools and processes necessary to implement that support, operations and maintenance plan;
6. Development of an implementation methodology, including, among others, automated deployment technologies, and installation instructions written to the appropriate level of the installer;
7. Preparation of an operational acceptance test plan, an integration design document, an implementation plan, and a support plan ready for review and approval by the NRC;
8. Preparation of final end-user documentation ready for NRC approval.;
9. Preparation of a proposed implementation sub-project schedule ready for NRC approval;
10. Development of any required training support for the end users;
11. Run a limited pilot test to determine any functionality and integration issues and to validate the implementation and support methods. Support for this pilot will be by a specially selected cross functional group of all support tiers and the development team;
12. Implementation and testing of the INMS tools for monitoring, maintenance and reporting of the new technology and related changes required to any existing systems;
13. Creation of a detailed Operational Acceptance Test plan;
14. Issues and bug tracking method determined and user feedback mechanism defined;
15. Approval of the detailed Operational Acceptance Test plan by all stake holders.

5.6 Operational Acceptance Testing

The purpose of the operational acceptance testing phase is to ensure that the implementation method works and that the new technology, as installed on the POE, will be stable, reliable, and supportable and provide the functionality specified in the analysis.

Before the operational acceptance testing can begin, the integration into the POE must be completed. Documentation from the integration into the POE phase can be in draft format, as it will be tested and improved during operational acceptance testing.

The goal of the operational acceptance testing phase is a fully operational test system on the NGN installed by a working implementation method and a list of known problems and issues which can be resolved during the transition to support.

The steps of the operational acceptance testing phase are:

1. The implementation method is performed by the installers on a test system on the NGN;

2. Reliability and workstation compatibility tests are performed within the network environment;
3. Compatibility tests with the Next Generation Network (NGN) components of the POE are performed. These include tests of functionality on the network, network operating system, and operating systems of the NGN, and functionality of all data exchange and other interfaces with POE applications, operating systems, and hardware;
4. End-user testing is performed;
5. Other tests, such as crash recovery tests, as specified in the Operational Acceptance Testing Plan, are performed;
6. If any minor problems are found, they are resolved by the developers from the integration development team and the tests are run again, as many times as needed until the tests are passed;
7. If any major problems are found, the new technology is returned to Phase 6, integration into the POE for rework;
8. If any changes are made, all technical test series are re-run. End-user tests are double checked, but do not need to be run at full capacity. Version control is in place;
9. Documents, such as installation and user guides, are also tested during operational acceptance testing. They are edited and final drafts are prepared;
10. An expanded pilot test is initiated encompassing a larger cross section of users and a larger portion of the support group in operations as well as the development team; and
11. Once the new technology has passed all tests, it is approved for transition to support, and implementation and training;

CM/RM

12. Configuration Management reviews all documentation;
13. Release Management reviews all documentation and deliverables;
14. Release Management process commences;
15. Configuration Management approves new technology as part of a release package for implementation and approves package deployment start date.

5.7 Transition to Support

The purpose of the transition to support phase is to ensure that all support teams are fully prepared to support the new technology on the POE and move the development team away from the operations, support, and maintenance of the new technology.

Before the transition to support can begin the integration into the POE must be completed.

The goals of the transition to support phase are:

- Finish the training and indoctrination of all support staff;
- Ensure that all monitoring and management systems are in place and functioning correctly in accordance with the support, operations and maintenance plan;
- Begin the training of the main user population; and
- Confirm that all documentation is complete and approved.
- Release management process begun.

The steps of the transition to support phase are:

1. Implementation Schedule prepared and submitted for approval;

2. Completion of any outstanding documentation, documentation and any outstanding final approvals;

3. Regular meetings between the development team and Network Operations are held, maintaining an Open Issues document, and working until all open issues are resolved;
4. Complete training and certify the NOC staff members in installation (if applicable) and support of the new technology;
5. Complete training and certify CSC staff members in installation and customer support of users of the new technology;
6. Issues and bug tracking processes are used to resolve problems as quickly as possible;
7. Integration of lessons learned into documentation and product. NOC and CSC staff participate in finalizing any document or new technology changes;
8. Approval of the final implementation schedule.

5.8 Implementation and Training

The purpose of the implementation and training phase is to deliver the new technology to users on the POE so that they can use it. If end-user training is provided, it is offered on a coordinated schedule with implementation.

Before the implementation and training phase can begin the transition to support must be completed.

The goal of the implementation and training phase is a production system of the new technology on the POE supported by the NOC and CSC.

The steps of the implementation and training phase are:

1. A meeting with departmental Information Technology Coordinators to introduce the new technology and plan details of implementation and introduction of the technology to users;
2. Bulletins and other memoranda and notices informing users of the implementation schedule to their departments;
3. Implementation to all parts of the NGN and POE receiving the new technology;
4. Implementation of full support of the new technology by the NOC and CSC, and the end of routine support by the ITID/IDIB consulting team. This includes final preparation of NOC and customer support SOPs and training of all NOC and CSC staff;
5. Receiving and integrating user response to the new technology;
6. End-user training, if any, coordinated with deployment to users in each department; and
7. A build-fix cycle that ensures that any problems that arise during implementation are identified, resolved, and deployed to (a) the system that reported the problem, (b) other systems which have already been deployed, and (c) systems that are going to be deployed;
8. User feedback mechanism in place;

RM/CM

9. Update Configuration Management Databases as new technology is deployed.

5.9 Operation and Support

The purpose of the operation and support phase is that, during the life of the new technology, it is used and provides benefit to the NRC and its staff. It is well-maintained at low cost.

Before the operation and support phase can begin the transition to support and implementation and training phases must be completed.

The goal of the operation and support phase is many useful, low cost years of life for the new technology.

The steps of the operation and support phase are:

1. Ongoing support of the application by the NOC;
2. Ongoing support of users by the CSC;
3. Over the first few months, close review of problems that arise. This review may lead to additional NOC/CSC training, and/or a new IDPM cycle for improvement of the application;
4. Verification that support SOPs and escalation SOPs are being followed by the NOC and CSC, and determination of the validity of these SOPs. SOPs will be re-written if necessary;
5. Maintenance of any vendor or consulting support contracts needed for the new technology;
6. Installation or re-installation of the new technology as needed to support growth or changes of use of the new technology;
7. Maintenance of the integration of this technology with system and usage changes and POE security;
8. Integration of other new technologies with the technology that has been implemented, through other IDPM cycles;
9. Issues, bug tracking, long-term trending using INMS and help desk tracking software are used to determine how effective cost-reduction or increased value of usage can be obtained;
10. Identification of the need for minor changes, major changes, or replacement of the technology.

5.10 Decommissioning and Disposal

The purpose of the decommissioning and disposal phase is the proper ending of the use of the technology in place with its replacement with a newer technology implemented through the IDPM process.

Before the decommissioning and disposal phase can begin, the NRC must recognize that this component of the POE has reached the end of its useful life.

The goal of the decommissioning and disposal phase is the secure and cost-effective removal of the technology from the POE as the technology that functionally replaces it is phased in through a new IDDM.

The steps of the decommissioning and disposal phase are:

1. Determination of the date of the end of the useful life of the technology;

2. Creation of a decommissioning plan which addresses security, equipment, licensing, and usage issues;
3. Creation of a new IDPM cycle for a new technology which will functionally replace the existing technology;
4. Implementation of the new technology;
5. Assurance of the functionality of the new technology;
6. Decommissioning of the old technology, so that it is turned off and no longer accessible to users;
7. Check to ensure all users can perform all tasks on the POE without this technology present;
8. Confirmation that all data on the old technology has been transferred to the new technology;
9. Secure elimination of data on the old technology;
10. Identification of alternate uses of equipment, and disposition of that equipment to alternate locations, or sale, donation, or disposal of that equipment;
11. Upgrade, transfer, or cancellation of software licenses, as appropriate; and
12. Upgrade or termination of support contracts, as appropriate;

RM/CM

13. Update Configuration Management Databases as decommissioning progresses.

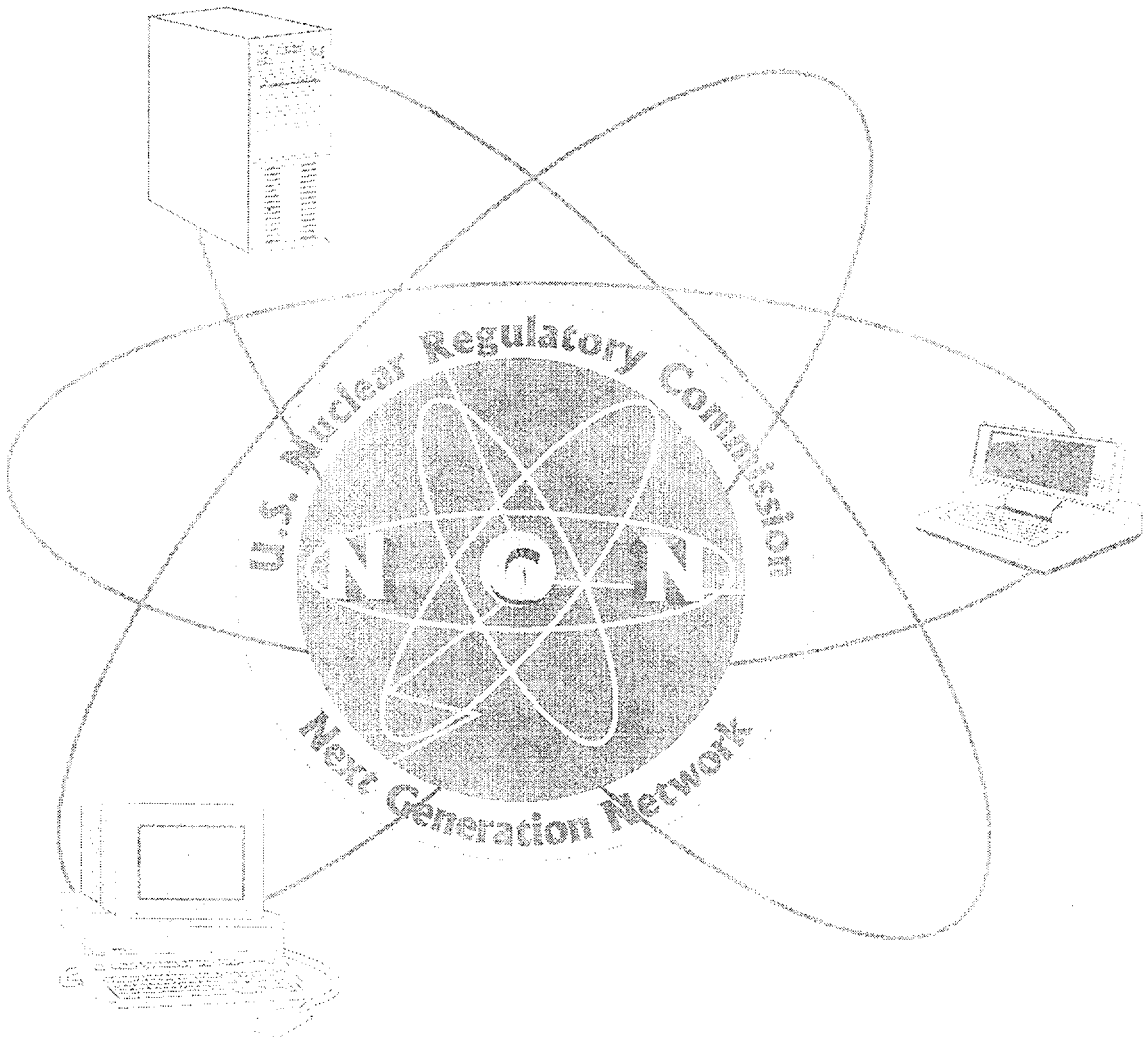
Attachment A - Generic Primavera Schedules for all Ten Phases

TITLE	ES	EF	OD
INFRASTRUCTURE DEVELOPMENT PROCESS MODEL	02-Jan-01_)	14-Jun-01_)	117
Phase I - Detailed Requirements Analysis	02-Jan-01_)	18-Jan-01_)	13
Start	02-Jan-01_)		0
Recognition of a need	02-Jan-01_)	02-Jan-01_)	1
Creation of a Task Order	03-Jan-01_)	09-Jan-01_)	5
Meeting w/ NRC users/technical staff def. req.	10-Jan-01_)	10-Jan-01_)	1
Analysis of affected, created, or eliminated	11-Jan-01_)	17-Jan-01_)	5
Identify other users affected by new tech	18-Jan-01_)	18-Jan-01_)	1
Phase II - Detailed Design Phase	19-Jan-01_)	26-Jan-01_)	6
Identification of technical teams involved	19-Jan-01_)	19-Jan-01_)	1
Creation of detailed functional specs.	22-Jan-01_)	22-Jan-01_)	1
Preparation of a detailed conceptual design	23-Jan-01_)	23-Jan-01_)	1
Determination of type of project: new SW/HW...	24-Jan-01_)	24-Jan-01_)	1
Determination of size of project: small/large	25-Jan-01_)	25-Jan-01_)	1
Determination whether new tech purchased/custo	26-Jan-01_)	26-Jan-01_)	1
Phase III - New Technology Development	29-Jan-01_)	27-Feb-01_)	21
Review of the technical design	29-Jan-01_)	29-Jan-01_)	1
Determination of roles of all stakeholders	30-Jan-01_)	30-Jan-01_)	1
Selection of vendors and consultants	31-Jan-01_)	31-Jan-01_)	1
Purchase of components	01-Feb-01_)	01-Feb-01_)	1
Assembly of the system	02-Feb-01_)	02-Feb-01_)	1
Custom integration	05-Feb-01_)	05-Feb-01_)	1
Changes to the technical design, as needed	06-Feb-01_)	06-Feb-01_)	1
Preparation of User Guide	07-Feb-01_)	07-Feb-01_)	1
Review of POE that new tech will interact w/	08-Feb-01_)	08-Feb-01_)	1
Preparation/approval of test plan	09-Feb-01_)	09-Feb-01_)	1
A determination of feasibility	13-Feb-01_)	13-Feb-01_)	1
Internal testing	14-Feb-01_)	14-Feb-01_)	1
Production of an analysis document	15-Feb-01_)	27-Feb-01_)	9
The project name	15-Feb-01_)	15-Feb-01_)	1
Description of the scope of project	16-Feb-01_)	16-Feb-01_)	1
The primary user's detailed needs requirements	19-Feb-01_)	19-Feb-01_)	1
Secondary user's detailed needs requirements	20-Feb-01_)	20-Feb-01_)	1
List parts of POE affected by new tech	21-Feb-01_)	21-Feb-01_)	1
Description of parts of POE requiring design	22-Feb-01_)	22-Feb-01_)	1
Initial draft project budget and schedule	23-Feb-01_)	23-Feb-01_)	1
Approval of detailed requirements analysis doc	26-Feb-01_)	26-Feb-01_)	1
Approval of funding for design phase	27-Feb-01_)	27-Feb-01_)	1
Phase IV - New Technology Acceptance Testing	28-Feb-01_)	29-Mar-01_)	22
Approval of functional specs./conceptual design	28-Feb-01_)	28-Feb-01_)	1
Prep. of tech. designs w/ product specs. time	01-Mar-01_)	01-Mar-01_)	1
Prep. of comparison chart/recomm. alternatives	02-Mar-01_)	02-Mar-01_)	1
A go/no go decision of entire project	05-Mar-01_)	05-Mar-01_)	1
Selection of tech. design options approved	06-Mar-01_)	06-Mar-01_)	1

TITLE	ES	EF	OD
Budget approval for remaining eight phases	07-Mar-01_)	07-Mar-01_)	1
Inform stakeholders of delivery date	08-Mar-01_)	08-Mar-01_)	1
Creation of the transition	09-Mar-01_)	09-Mar-01_)	1
Form a test group	12-Mar-01_)	12-Mar-01_)	1
Stakeholders review Acceptance Test Plan	13-Mar-01_)	13-Mar-01_)	1
Acceptance Test Plan is set up	14-Mar-01_)	14-Mar-01_)	1
Identify users to participate, if desirable	15-Mar-01_)	15-Mar-01_)	1
Testers set up test environment/install new tec	16-Mar-01_)	16-Mar-01_)	1
User tests are performed	19-Mar-01_)	19-Mar-01_)	1
Initial creation of INMS monitoring/support	20-Mar-01_)	20-Mar-01_)	1
Compatibility tests w/ NGN components of POE	21-Mar-01_)	21-Mar-01_)	1
Perform other tests: load/stress/functionality	22-Mar-01_)	22-Mar-01_)	1
Resolve minor problems, if found	23-Mar-01_)	23-Mar-01_)	1
Major problems found, return to phase IV	26-Mar-01_)	26-Mar-01_)	1
If any changes made, test series are re-run	27-Mar-01_)	27-Mar-01_)	1
Approved for integration into POE	28-Mar-01_)	28-Mar-01_)	1
Integration into the POE	29-Mar-01_)	29-Mar-01_)	1
Phase V - Integration into the POE	30-Mar-01_)	16-Apr-01_)	12
Develop detailed sub-project schedule	30-Mar-01_)	30-Mar-01_)	1
Determination of optimal deployment methods	02-Apr-01_)	02-Apr-01_)	1
Resolve all remaining compat/reliab. issues	03-Apr-01_)	03-Apr-01_)	1
Creation of a support plan	04-Apr-01_)	04-Apr-01_)	1
Development of an implementation methodology	05-Apr-01_)	05-Apr-01_)	1
Preparation of operational accept. test plan	06-Apr-01_)	06-Apr-01_)	1
Preparation of final end-user documentation	09-Apr-01_)	09-Apr-01_)	1
Preparation of implem. sub-project schedule	10-Apr-01_)	10-Apr-01_)	1
Develop required training support - end users	11-Apr-01_)	11-Apr-01_)	1
Run a limited pilot test	12-Apr-01_)	12-Apr-01_)	1
Creation detailed Operational Accept. Test plan	13-Apr-01_)	13-Apr-01_)	1
Approval of Operational Test plan by stakehold	16-Apr-01_)	16-Apr-01_)	1
Phase VI - Operational Acceptance Testing	17-Apr-01_)	27-Apr-01_)	9
Implementation method performed by installers	17-Apr-01_)	17-Apr-01_)	1
Reliability/Compatibility tests performed	18-Apr-01_)	18-Apr-01_)	1
End-user testing is performed	19-Apr-01_)	19-Apr-01_)	1
If any minor problems found, resolved by devel	20-Apr-01_)	20-Apr-01_)	1
If major problems found, return to phase VI	23-Apr-01_)	23-Apr-01_)	1
If changes made, re-run test series	24-Apr-01_)	24-Apr-01_)	1
Documents tested edited, and final prepared	25-Apr-01_)	25-Apr-01_)	1
Expanded pilot test is initiated	26-Apr-01_)	26-Apr-01_)	1
Tests passed approved for Transition to support	27-Apr-01_)	27-Apr-01_)	1
Phase VII - Transition to Support	30-Apr-01_)	03-May-01_)	4
Completion of documentation	30-Apr-01_)	30-Apr-01_)	1
Regular meetings of the transition team	01-May-01_)	01-May-01_)	1
Complete training/certify NOC staff members	02-May-01_)	02-May-01_)	1

TITLE	ES	EF	OD
Incorporate lessons learned in documentation	03-May-01_)	03-May-01_)	1
Phase VIII - Implementation and Training	04-May-01_)	16-May-01_)	9
Approval of final implementation schedule	04-May-01_)	04-May-01_)	1
Meeting w/ department Info. Tech. Coordinators	07-May-01_)	07-May-01_)	1
Inform users of implementation schedule	08-May-01_)	09-May-01_)	2
Implementation of all parts of NGN and POE	10-May-01_)	10-May-01_)	1
Implementation of full support of new tech.	11-May-01_)	11-May-01_)	1
Reviewing and integrating user response	14-May-01_)	14-May-01_)	1
End-user training, if needed	15-May-01_)	15-May-01_)	1
A build-fix cycle	16-May-01_)	16-May-01_)	1
Phase IX - Operation and Support	17-May-01_)	28-May-01_)	8
Ongoing support of application by NOC	17-May-01_)	17-May-01_)	1
Ongoing support of users by the CSC	18-May-01_)	18-May-01_)	1
Review problems that arise	21-May-01_)	21-May-01_)	1
Verification that support SOPs	22-May-01_)	22-May-01_)	1
Maintenance of vendor or consulting support	23-May-01_)	23-May-01_)	1
Integration of any other new technology	24-May-01_)	24-May-01_)	1
Long-term trending using INMS and help desk SW	25-May-01_)	25-May-01_)	1
Identification of need for minor/major changes	28-May-01_)	28-May-01_)	1
Phase X - Decommissioning and Disposal	29-May-01_)	14-Jun-01_)	13
Determine date of end of useful life of tech.	29-May-01_)	29-May-01_)	1
Creation of decommissioning plan	30-May-01_)	30-May-01_)	1
Creation of new IDPM cycle for new tech.	31-May-01_)	31-May-01_)	1
Implementation of the new technology	01-Jun-01_)	01-Jun-01_)	1
Assurance of functionality of new tech.	04-Jun-01_)	04-Jun-01_)	1
Decommissioning of the old tech.	05-Jun-01_)	05-Jun-01_)	1
Check to ensure all users can perform all task	06-Jun-01_)	06-Jun-01_)	1
Confirm all data on old tech has been transfer	07-Jun-01_)	07-Jun-01_)	1
Secure elimination of data on old tech.	08-Jun-01_)	11-Jun-01_)	2
Identification of alternate users of equipment	12-Jun-01_)	12-Jun-01_)	1
Upgrade, transfer, cancellation of software	13-Jun-01_)	13-Jun-01_)	1
Upgrade or termination of support contracts	14-Jun-01_)	14-Jun-01_)	1
Finish		14-Jun-01_)	0

Consolidated Test Facility
Concept of Operations



March 2, 2001

Table of Contents

1.0 Executive Summary 1
- 1.1 Attributes of the CTF 1
- 1.2 Process 2
  - 1.2.1 Research 2
  - 1.2.2 Development 2
  - 1.2.3 Testing and Integration 3
  - 1.2.4 Production 3
  - 1.2.5 Retirement 3
- 1.3 Requesting CTF Services 3

2.0 Executive Conclusion 4

3.0 Approach and Assumptions 5

4.0 Test Considerations (Technical Details) 7
- 4.1 General Requirements 7
  - 4.1.1 Application 7
    - 4.1.1.1 Application Layer Requirement 7
    - 4.1.1.2 Presentation Layer Requirement 7
    - 4.1.1.3 Session Layer Requirement (Workstation) 8
  - 4.1.2 Infrastructure 8
    - 4.1.2.1 Session Layer Requirement (Server) 8
    - 4.1.2.2 Transport Layer Requirement 8
  - 4.1.3 Network 9
    - 4.1.3.1 Data Link Layer Requirement 9
    - 4.1.3.2 Physical Layer Requirement 9
  - 4.1.4 Troubleshooting 9

5.0 Technical Considerations 9
- 5.1 ITID Network Operations Group 9
- 5.2 ITID Development Group 10
- 5.3 Application Development Division 11
- 5.4 NRC NGN Network Users 12

6.0 Summary 12

1.0 Executive Summary

As the NRC's dependency on its information technology infrastructure, and on the critical nature of the applications that use this infrastructure increases, the stability and security of the NRC network has become critical in ensuring the ability of the NRC to operate and to achieve its mission requirements. The increasing complexity and interactions between the various network infrastructure and applications components have made it nearly impossible to predict the behavior of major changes or application implementations, without actual testing in a representative environment. Furthermore, development efforts independently conceived and executed by NRC offices have encountered significant difficulties when attempting to integrate their system into the NRC WAN. This is due primarily to the lack of early-on development testing in a representative environment.

The NRC Consolidated Test Facility (CTF), therefore, will be a collection of hardware and software that represent the current production operational network environment at the NRC as well as providing a development testing environment . The CTF will be engineered such that the services and characteristics of the CTF will simulate both the current operational environment (for production testing) and an environment specifically aimed at supporting development testing. The goal of the CTF is to provide an environment where new hardware, software, services and applications can be tested and demonstrated prior to their release into the Production Environment, and, provide an environment where developers can perform in-depth testing and evaluation and have access to state-of-the-art systems for future development efforts. These objectives and processes are closely tied to the NRC's current System Development and Life Cycle Management model (SDLCM), Infrastructure Development Process Model (IDPM) and the Release Management Process. The environment will be constructed by the Information Technology Infrastructure Division (ITID) and operated by the IT Customer Service Branch (CSB). Applications Development Division (ADD). Stakeholders in the CTF are ITID, IMD, ADD, PRMD, and the users of the NRC NGN Network.

1.1 Attributes of the CTF

The CTF will be constructed to possess the following attributes;

- Flexible environment.
- Highly reconfigurable.
- Robust and resilient.
- Capable of representing the NRC environment and sub components.
- Capable of hosting multiple simultaneous testing activities.
- R&D Evaluations

In addition, the CTF will provide an environment for the following types of development and testing activities:

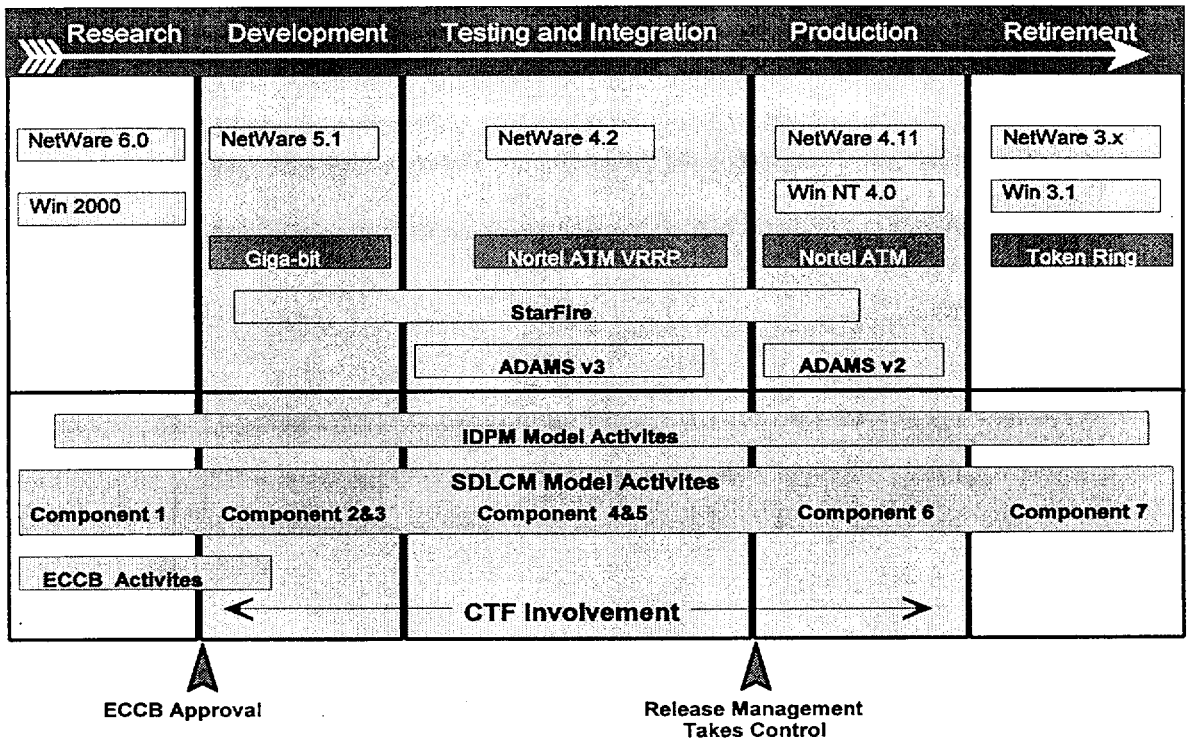
- **One Time Dev and Test-** These are efforts focusing on a single deliverable that is not expected to be upgraded or supported beyond its initial form.
- **Periodic Dev and Test-** These are efforts that have significant stable periods between changes or upgrades- i.e Network OS, Desktop OS (platform), etc.

- **On Going Dev and Test-** These efforts pertain to long term systems and applications which require routine updates, upgrades or changes. This would include Web development, desktop OS enhancements, service packs, etc.

1.2 Process

The following figure shows the overall process and where and how the CTF will be used during different stages of the development life cycle. The diagram shows current active projects as actual examples and places them in their appropriate stage. In addition, the bottom half of the model is overlaid with the ECCB, IDPM and SDLCM models illustrating their influence on the process. Note that the StarFire project is shown spanning three categories. This is not a normal condition for application development, but StarFire's scheduling constraints has allowed it to extend its R&D efforts into the production environment.

Figure 1



1.2.1 Research

The CTF will not normally be involved in the early stages of research. Research involves performing needs analysis, requirements analysis, presenting a business case, etc. This activity is dominated by the ECCB. It is after passing the ECCB requirements that the CTF will be used to identify solution candidates.

1.2.2 Development

Once a solution candidate has been identified, the CTF will be used to host development operations. Due to the flexible nature of the communications architecture, the CTF will have the

ability to extend its infrastructure out to various floors in both TWFN and OWFN. This will allow initial development efforts to take place elsewhere (people and equipment) while still providing all of the functionality and benefits of the CTF.

When a solution candidate has been developed sufficiently, it will then proceed to Testing and Integration.

1.2.3 Testing and Integration

This is the critical point in a system development cycle. This is when it is tested against the mock-up production environment. A system is tested not only for its functional attributes, but also for compatibility with the existing NRC WAN systems. The system would have been exposed early in development to the standard NRC environment (desktop OS, clients, NOS, etc), but this stage checks for its integration process (how it installs) and it functions with incumbent NRC applications (ADAMS, StarFire, RIMS, etc).

Systems failing at this stage return to Development for further investigation. Sometimes the problems are simple and can be resolved easily. Other times, the problems are more fundamental and require significant research. Systems passing this stage enter the Release Management Process and are scheduled for roll out.

1.2.4 Production

The CTF will become involved with production systems only if operational problems arise requiring a facility that can reproduce and test solutions. While this may not happen often, when it does, having a facility that can reproduce the environment and, more importantly, reproduce the problem, will greatly improve the chances for a quick and accurate solution.

1.2.5 Retirement

The CTF will most likely not be involved with the retirement of an application or system unless the process for removing the system requires testing.

1.3 Requesting CTF Services

The CTF suite of services include the following:

Research
Feasibility tests
Product evaluation
Vendor tests
Presentations

Development
Performance tests
Platform tests
Black Box tests
White Box tests
Code and Unit tests

Testing and Integration
Compatibility tests
Installation tests
Baseline product performance
Configuration tests

Production
Operational tests
Troubleshooting
Root cause analysis
Alternative solutions

Scheduling any or all of these services must be coordinated with the CTF Facilities Manager. Before requesting CTF services, the applicant must prepare a schedule identifying the types of CTF services required and expected duration. Applicants requesting the CTF host their systems will need to provide power, space and heat data along with the functional requirements. In addition, use of the test PC's must be conducted with an approved Test Plan (approved by ECCB, SDLCM and IDPM). As the number of test PC's is limited, applicants may choose to conduct early testing using PC's outside the CTF (facilitated by extending the test infrastructure to the developers area). Details of CTF scheduling and management are covered in more detail in the CTF Testing and Evaluation Process Plan (TEPP).

2.0 Executive Conclusion

For the Network Operations Group of ITID, the CTF will provide an environment that is as close as possible to the actual production network. This lab will provide the Operations group with the capabilities to model the behavior of network productions changes without placing the production network at risk from the changes in accordance with Section 5.6 of the IDPM and Sections 5.1.3 and 5.1.4 of the Release Management Process. The CTF will mimic both the infrastructure and the application environment to provide the most accurate data possible to the testers. Configuration of the CTF will be linked to Configuration Management for its configuration and will feed configuration data forward to the Operations Group and the Configuration Management System.

The lab will include all of the test equipment and tools necessary for measuring the effects of the changes in the lab. In addition, it will contain the tools needed for providing a load similar to that of the production network. The lab will conduct training on the new system for support personnel involved in the transition and deployment. An important secondary purpose for the lab is for troubleshooting and root cause analysis of network problems and outages.

For the Development Group of ITID, in accordance with IDPM Section 5.6 and Release Management Process Section 5.1.3., the CTF will provide an environment comprised of a complete infrastructure reproduction from Production environment plus a robust and highly flexible communications infrastructure capable of extending the resources of the CTF beyond the confines of the physical room. This last capability represents perhaps the most important aspect of the CTF. Developers, historically, have had to acquire all of the equipment necessary for the creation and testing of their projects. To that end, little or no development funding was ever diverted to acquire systems necessary for pre-production testing. In addition, developers work areas have usually been collocated with their development systems. The CTF will offer, for the first time, the ability to grant developers an isolated, independent link to the CTF (regardless of their physical location) and to all of the capabilities therein. The CTF and the testing of any new systems or changes comprises the test and acceptance where control of a project is transitioned from development to operations. The systems tested in the CTF must meet the required criteria, as set forth in the IDPM, and will be constructed to provide the required data along with the management capability to monitor and test the management integration of the new system. The CTF design will also incorporated a new systems capacity testing capability.

For the ADD, the CTF will serve as a mid and late term development point where their systems may be introduced to the mock NRC WAN infrastructure much earlier than in the past. This early exposure to the mock NRC WAN will serve to uncover conflicts and/or additional system requirements that would have otherwise gone undetected until production release. The CTF

will then become the transition point for the appropriate parts of the SDLCM into the ITID IDPM and Release Management Process that is common to all of the models. The testing and development capabilities of the CTF will determine the impact of the new software on the operational environment and its components while measuring the effects of the operational components on the new application. The developers will be able to test their products in the CTF against the requirements of the downstream consumers of their development products with the focus being on production rather than development. Late term development testing in the CTF will allow the development staff to be able to test in an environment that is closest to the operational environment, thus eliminating the need for multiple smaller test environments that do not accurately match the production operation.

For the NRC users, the CTF will serve as a laboratory for previewing new systems and applications before they are released. This environment will be beneficial for applications that have user interface and/or customization issues or steps that are yet to be resolved. The CTF will be constructed such that portions of it can be reconfigured from test area to class or demonstration area. This provides the ideal environment in which to showcase systems and applications as well as resolve issues before the application is transitioned into the Release Management Process.

3.0 Approach and Assumptions

The following assumptions have been made regarding the design and function of the CTF:

1) It will be located on the 2rd Floor of TWFN at the Technology Center site, not including the associated space behind the back wall of the center;

2) It is not currently part of, or involved with the planned ADAMS Disaster Recovery Site to be installed at the Sytel NGN Contract Office in the Rockwall One building;

3) The CTF will have the greatest degree of flexibility and expandability built into it;

4) The CTF will provide the equipment to monitor and analyze performance, as well as provide a test bed for data and performance recording and stress testing;

5) All testing in the CTF will be managed by ITID.

The approach used to design and construct the CTF will be a collaborative effort between the three OCIO stakeholders. The ITID Development Group will be responsible for most of the design and the initial implementation of the CTF. The CTF must be flexible enough to model all possible configurations in the Configuration Management Database. The Production side of the CTF will be modeled closely on the existing NRC NGN Network with some very important additions. The network management system for the CTF must have the added capacity to support the multi-layered testing that will occur in the CTF. There is no single product that will be able to provide all of this functionality. In addition, several other supplemental systems that are not part of the operational environment will need to be specified. Including the management augmentation, systems that can provide a simulated load for testing capacity, performance and stress capabilities will be required. The ITID Operations Group will insure that the Production side of the CTF meets the specific technical requirements of the ITID Network Operations Group for IDPM, SDLCM and Release Management Process compliance. The Operations Group will also validate that the management system used in the CTF conforms to

the standards, practices, and processes found in the management system used in the operational environment.

ITID will also oversee the design and construction of the Development side of the CTF. The requirements for supporting all development needs by all stakeholders are still being acquired. However, there are fundamental components of a development environment that can be identified now. These are:

- A complete duplication of the infrastructure and applications systems present in the Production side of the CTF. This will allow developers to perform early testing with their systems and permit changes to both their system and the NRC Infrastructure when performance issues arise.

  Example: If, during mid term development testing, a performance issue is discovered, the developers will have the ability to adjust not only their system, but also to make changes to the infrastructure such as increasing link speeds or changing the host systems.

- A significant number of state-of-the-art server platforms for use by developers. These would include individual servers as well as manufacturer provided advanced systems including SANs, server clusters, cache servers, etc.

  Example: A developer wishes to determine if clustering would improve overall response time with respect to their particular system. The CTF would have servers on hand that could be easily configured and made available at no additional cost to the developers.

- Adequate open floor space in the CTF Computer Center for developers to locate their host systems during mid and late term development testing. This would also serve as the transition point to Production testing.

  Example: A developer has completed the early stages of system development independent of the CTF facility. They now wish to make use of the load testing and performance measuring capabilities of the CTF. They can relocate their system to the CTF where it is integrated into the NRC mock environment.

- A communications infrastructure that can be extended out to any floors in OWFN and TWFN. This would allow the CTF to be accessed by developers without them having to be physically in the CTF.

  Example: A developer has 15 people working on a project. It would be difficult to accommodate that many people for a long period of time in the CTF. However, by creating a VLAN and extending it, via independent cabling, to the developers location, and development PC's could be directly connected back to the CTF and they would have access to everything in the CTF without leaving the floor.

The ADD will: 1) determine application specific infrastructure requirements and, 2) provide the application components, documentation and training required to install and maintain agency-wide or agency critical applications installation and maintenance.'

4.0 Test Considerations (Technical Details)

4.1 General Requirements

The requirements for the CTF are very logical and follow directly from the CTF development purpose and can be formed into four general requirements that can be broken down further into specific requirements. From these special requirements, a bill of materials for the test lab can be produced, standard operating procedures created, and processes implemented to obtain the maximum cost-effectiveness from the investment in the lab. Four general requirements have been identified: 1) Application, 2) Infrastructure, 3)Network, and 3) Troubleshooting. These general requirements can be divided further into levels that roughly coincide with the Open Systems Interconnection Reference Model (OSI RM).

4.1.1 Application

This general requirement concerns the network end-user nodes that are located at the edges of the network and uses the services provided by the network to perform various functions. The CTF will contain all of the critical agency applications in a form that can be used to simulate the actual operation of the application in the Production Operations Environment. This will allow for detailed studies of new applications and their interactions with the existing applications, as well as the underlying infrastructure. The CTF will also provide mechanisms for testing changes to existing infrastructure and application components, and the effects of those changes in the overall environment. This requirement is vital as more and more agency-wide, critical applications are implemented, and as resources and services become limiting factors to the implementation and performance of these new applications.

Determining the load that an application places on the workstation and a user level perception of performance are two of the key quantitative and qualitative measurements, respectively, that are performed at these layers. Another point of interest is the efficiency of the application in requesting, using and releasing workstation resources as they are needed and adherence to standards and/or tools that are specified to be used on the NRC workstations and network.

4.1.1.1 Application Layer Requirement

On the uppermost layer of the OSI RM, the requirement will be to test and evaluate applications and changes to applications from the perspective of the user. Response time testing, compatibility, and overall stability will be the primary test requirements for this layer. Response time and stability are important user issues that can cause an increase in support costs due to user frustration and perceived application failures.

4.1.1.2 Presentation Layer Requirement

In this layer, the client software that supports the applications is grouped together. This will include ODBC clients, application specific services or processes (or new/non-standard operating system services or processes required to run the application), transaction processors, etc. The requirements at this layer will be efficiency, speed and stability. The primary goal of

the requirement is to achieve user oriented satisfaction, however, there are other requirements for compatibility and efficient use of workstation resources.

4.1.1.3 Session Layer Requirement (Workstation)

This requirement is divided between the application and infrastructure general requirements. This allows for flexibility in testing n-tiered applications that may have portions running on the workstation or on a server(s). For this application, items such as local data stores and caches or component objects not related directly to the GUI or top level application module(s), and similar objects. The main requirements at this layer will be interface reliability and semantic consistency. Another important requirement will be the service requirements from the server based portions of distributed objects and components at this layer.

4.1.2 Infrastructure

This general requirement concerns the devices at the edge of the network that provide connectivity from the workstations to devices at the backbone of the network which provide the services and connectivity to the network components. The test lab will contain enough equipment to provide a complete miniature model of the NRC network, such that all aspects of network functionality and impact can be assessed whenever a new component is added to, or an existing component is modified on the network. Therefore, detailed study and quantitative analysis concerning the impact of these changes or additions to the Production Operations Environment can take place. The requirements will be to assess the load placed on the network components, stability and security of the network after specific changes, including the effect on shared services, components, and servers. Many of the test requirements, such as overall traffic loads, will be transferable across many layers, whereas some of the testing requirements will be confined to the behavior of the addition or change at that specific layer only, for example - port and service access usage.

4.1.2.1 Session Layer Requirement (Server)

This requirement is the second half of the session layer requirement for the application general requirements. This requirement's focus is on the servers and the effects of changes on them, both to their physical capabilities and to the services they provide. The range of components at this level, however, are more varied than at the workstation level. These components can include database engines, e-mail services, transaction processing, file services, distributed objects, print services, and authentication services, to name a few. The requirements at this layer will be concerned with loads on the services that are provided by the servers and potential consequences of new services being added to the server and their effects on existing services. Additionally important are the interfaces with other server based services and complementary workstation components.

4.1.2.2 Transport Layer Requirement

This layer's requirements are focused mainly on interface consistency and connection management. Interface requirements will include verification of proper service access configuration. The connection requirements will determine application requirements on connections and connection buffers. Although testing at this layer is very narrow and specific, it

is vital to insure that the communications resources of the network components will not be oversubscribed, therefore, causing lost connections and data, and that data is sent to the correct service access points for processing at upper layers. As policy based networking is introduced into the NRC network, policy testing and enforcement of policy requirements will add to the testing load of this layer.

4.1.3 Network

Requirements for testing at this layer may vary quite a bit depending on the new component or change and its position in the network. Requirements for testing routing compatibility and multi-cast group management may also be necessary. Key testing requirements will included ensuring that the most efficient use of network protocols has been achieved and that this use conforms to NRC standards for network protocols and services.

4.1.3.1 Data Link Layer Requirement

The requirement at this layer will be limited strictly to components such as network interface card drivers and network transport components. The testing will be comprised primarily of the standards' adherence to verification and compatibility testing. Proper driver configuration and resource requirements will be confirmed to or adjusted so the optimal network requirements will be met.

4.1.3.2 Physical Layer Requirement

The requirements that would normally be associated with this layer are somewhat distant from the scope of testing in a CTF environment. Testing will be comprised mainly of conformation of adherence to NRC and interface standards. Testing requirements for bulk network load will be done at this level. This will be the main requirement and will determine the overall percentage of network bandwidth and resources that any addition or change will affect the network.

4.1.4 Troubleshooting

The final general requirement for the CTF will be for troubleshooting, problem duplication and root cause analysis purposes. The test lab will contain the required equipment to enable duplication of configurations and conditions that occur in the Production Operations Environment during periods of degraded performance or failure.

5.0 Technical Considerations

5.1 ITID Network Operations Group

In addition to the general considerations for the CTF, the ITID Network Operations Group has specific considerations and requirements that they will be focusing on in the CTF. The Operations Group has the primary responsibility for IDPM and Release Management Process enforcement. Section 5.6 of the IDPM, Operational Acceptance Testing, is the phase of the IDPM where the major control of a new or modified system transitions from development to the Operations Group. In order for this transition to take place the following criteria must be met:

1) *The implementation method is performed by the installers on a test system on the NGN is tested;*

2) *Reliability and compatibility tests are performed;*

3) *End-user testing is performed;*

4) *Other tests, such as crash recovery tests, as specified in the Operational Acceptance Testing Plan, are performed;*

5) *If any minor problems are found, they are resolved by the developers from the integration development team and the tests are run again, as many times as needed until the tests are passed;*

6) *If any major problems are found, the new technology is returned to the development organization for rework;*

7) *If any changes are made, all technical test series are rerun. End-user tests are double-checked, but do not need to be run at full capacity. Version control is in place;*

8) *Documents, such as installation and user guides, are also tested during operational acceptance testing. They are edited and final drafts are prepared;*

9) *An expanded pilot test is initiated encompassing a representative cross section of users and a larger portion of the support group in operations as well as the development team;*

Source: Infrastructure Development Process Model v1.1, Section 5.6, 31 JAN 2000

The CTF also serves as the training environment for Section 5.7 of the IDPM. For the Release Management Process, the new system or application is tested as part of a release package in the CTF, if applicable.

The ITID Operations group will be managing the CTF. This includes both the resources to schedule the testing, maintain the configurations and other activities in the CTF as well as the operation and maintenance of the CTF and the equipment contained within it. The level of effort that will be required for this is not trivial and should be considered before any designs are finalized. Design options and schematics should include the resource estimates for providing the management and operations functions in the CTF.

5.2 ITID Development Group

The ITID Development group has design oversight for the network infrastructure and the agency wide services that run over them. Infrastructure components include items such as switches, servers and routers and the firmware and software that runs on them. The services that they support include things such as the email system, Internet access and office automation software. The Development group is responsible for keeping the systems up to date and adding infrastructure components or services as the needs of the agency dictate. The ITID

Development Group uses the IDPM to identify, develop and deploy these additions as well as changes and updates. The IDPM outlines two major test phases, one that occurs at a development location that is used to confirm gross proper operation of the system and a second to verify that the system can be integrated into the Production Environment without causing harm to any of the components in the production environment.

One of the purposes of the CTF is to provide the test bed for the second test phase. It is the function of the ITID under the IDPM to insure that they are turning over a completed, functional product to the operations group to manage in accordance with IDPM section 5.6. In addition to a detailed, exhaustive test of the system, the ITID Development group is responsible for providing final configuration data to the Operations Group as well as providing the training required to bring the Operations Group up to the level of knowledge required to operate and maintain the system. Final configuration data will be collected at the end of the test, if the system is accepted by virtue of passing the tests successfully. This Configuration information will be entered into the Configuration Management Database in accordance with the Configuration Management Process. The CTF will also serve as the training system for the Development Group to train the Operations Group with. The CTF thus enables the final steps of development to be smoothly and efficiently turned over into the Operations Group.

In addition, through the effective use of the stress testing capabilities of the CTF, it will be possible to make network capacity requirement estimates based on many usage related factors. This information will be very useful in network planning and also provide thresholds that can be monitored to indicate when a system is about to 'outgrow' the current network infrastructure with enough warning so that the capacity issue can be dealt with pro-actively.

5.3 Application Development Division

The ADD of the NRC is the primary source for applications that run on the network infrastructure and make use of network services. Their first concern is in producing an application that meets the requirements of their client or clients and that the performance of the application, at the application layer, meets the requirements and expectations of the application users. In the CTF, ADD will have the capability to do final checks on functionality requirements as well as any interface customization may be necessary. Although any issues with the functional requirements of the application should be resolved by this point, the CTF serves as the final quality check before the application is released, saving costly rework further down the support chain. The application layer performance of the new system is the most important part of any application once the functional requirements are met. Good application layer performance is the hallmark of a well developed and efficient network application and the CTF will have all of the tools and facilities to confirm that the application layer performance is acceptable and will not change when the application is released into the Production Environment. The Application layer performance is very closely tied into many different factors. One factor that can have a large impact on application layer performance is the second ADD concern that the CTF addresses.

The second concern of ADD is that the applications should use a minimum amount of the network infrastructure while efficiently using network services. It is imperative that the application does not impair the network infrastructure or network services in any way. The CTF will provide the platform for testing that the application meets the requirements for efficiency while providing favorable services. The CTF, being configured to match the Production Environment, and having the management capability to examine the behavior of the infrastructure, services, and applications in detail, will provide the data required to confirm this.

The CTF is a bridge point between the SDLCM of ADD and the IDPM of ITID. The overriding concern of ADD is that the application that is implemented into the Production Environment is functional and does not harm the network. As with the ITID Development Group, ADD will be able to provide configuration data and training directly in the CTF for the ITID groups that require training to assume operations, maintenance and support functions for the new application.

5.4 NRC NGN Network Users

The CTF considerations for the users primarily target the part of the lab that will be used for demonstration and interface issues. New applications with customizable graphical user interfaces can be previewed in a number of different configurations and the users can help the developers to determine which particular configurations would best suit the user population. Including users in the interface design process increases the level of user buy-in with new applications, especially where it is an older accustomed application that is being replaced by something new and different.

Users who are primary stakeholders in applications can use the CTF to test application functionality and performance. The product developer can also perform other tests for the users to witness. Involving primary users before deployment better acquaints the users with the progress and correctness of the development project and can help to avoid redeployment and rework once the application has been fielded. User acceptance testing also increases user buy-in of the application.

6.0 Summary

The Consolidated Test Facility is an ideal point to focus the intersections of the ADD SDLCM and the ITID IDPM, Release Management Process and Configuration Management Process. It is the one point where development and operations share a responsibility to insure that there is not implementation of unknown factors on the network or anything that could cause damage to the Production Environment. The CTF is also instrumental in providing a training platform for operations, capacity planning thresholds and the final development of Graphical User Interface (GUI) configurations

SERVICE LE\ REQUIREMENTS

Core Service Bands General Purpose Desktop Environment				
Service Measurements	**VIP**	**Professional**	**RISE**	**Other (Remote, etc.)**
	CSBGPDT1	**CSBGPDT2**	**CSBGPDT3**	**CSBGPDT4**
Infrastructure Management Service Area (C.3.1)				
General Services				
Availability during the primary support period. (Number of hours of service availability divided by the number of hours in the primary support period, per month)	99%	97%	95%	93%
File, Print, Application Server Availability The average percentage of time each network server is fully available to the users. The percentage is calculated by dividing the sum of down times (hours down times the number of users affected) by the Total Hours of availability times the total number of users, minus the sum of the scheduled outages (the downtime of the outage times the number of affected users. See the note bellow for further detail	99.6%	99.6%	99.6%	99.6%
Network Throughput Throughput is the rate at which data is transferred through the network, expressed in Megabits per second (Mbps), and measured by counting the bytes transported during a specified period of time.	> 10 Mbps of data to the desktop	> 10 Mbps of data to the desktop	10 Mbps of data to the desktop	N/A
Network Bandwidth				
Scalability				
File Server Storage Volume The amount of space, measured in Megabytes (MB) available to each user in a network file server.	100MB per user	100MB per user	100MB per user	50MB per user
Electronic Performance Monitoring, Incident Detection, and Diagnostic Service (Provides automated incident or fault detection and response initiation. Applies to components which are powered up, operating, and network connected.)	Yes	Yes	Yes	Yes
Electronic Notification Service (Components which are powered up, operating, and network connected)	Yes	Yes	Yes	Yes
Electronic Software Distribution (Components which are powered up, operating, and network connected)	Yes	Yes	Yes	Yes
Electronic Topology/Configuration Management Includes Configuration Management for all DCE components: Current description of image, current configuration of hardware and software, current location Accessible by NRC	Yes	Yes	Yes	Yes
Performance Analysis and Tuning (Components which are powered up, operating, and network connected)	Monthly	Monthly	Monthly	Upon Request (Limit 4 per year)

Co ervice Bands General Purpose Desktop Environn				
Service Measurements	**VIP**	**Professional**	**RISE**	**Other (Remote, etc.)**
	CSBGPDT1	**CSBGPDT2**	**CSBGPDT3**	**CSBGPDT4**
Virus Scanning	Yes	Yes	Yes	Yes
IT Security Tracking Identify and track incident occurrence on NRC supported systems. Incidents to be tracked may include, but not limited to: unauthorized access of a NRC supported system wherein a valid account is used without authorization and successfully gains access to the system; a valid account is used in excess of authorized access and successfully gains access to unauthorized information; a weakness in the system is successfully exploited and successfully used to gain access to unauthorized information; resources are stolen which provide access to password files, protected or restricted data (proprietary or export controlled), licensed applications or software, restricted applications, software or code; or, an authorized account is used in violation of Federal or NRC policies regarding proper use of computer resources.	Yes	Yes	Yes	Yes
Security Incident Reporting Promptly report any suspected computer or network security incidents occurring on any systems. If it is validated that there is an incident, the Contractor shall provide all necessary assistance and access to the affected systems so that a detailed investigation can be conducted and lessons learned documented.	Within 15 minutes of incident occurrence	Within 15 minutes of incident occurrence	Within 15 minutes of incident occurrence	Within 15 minutes of incident occurrence
Network File Backup				
Local Drive Storage Backup To Network Data files in Standardized Directory only for components that are powered up, operating, and connected to the network.	Daily	Weekly	Weekly	None, User Duty
User Administration Services				
HELP DESK (C.3.3)				
General Services				
Primary Support Period (Hours x Days)	12x5	12x5	12x5	12x5
Primary Support Days	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.
Primary Support Hours (Local Customer Time)	6am - 6pm	6am - 6pm	6am - 6pm	6am - 6pm
Number of Calls or Incident Responses Included in Service During Primary Support Period.	Unlimited	Unlimited	Unlimited	Unlimited
Time To Answer Calls The time from when the customer make the last ACD selection (if required) until the call is answered by a live person.	15 Seconds	15 Seconds	15 Seconds	15 Seconds
Percentage of Calls Answered Within Stated Time From First Ring	90%	90%	90%	70%
Number of rings before Voice Mail responds during core hours	3	4	4	5
Percentage of calls going to Voice Mail during Core Hours (Time to Answer Calls)	4%	4%	4%	6%

Co ervice Bands General Purpose Desktop Environn				
Service Measurements	**VIP**	**Professional**	**RISE**	**Other (Remote, etc.)**
	CSBGPDT1	**CSBGPDT2**	**CSBGPDT3**	**CSBGPDT4**
Percentage of Abandoned Calls	3%	3%	3%	3%
Time to Respond to Other forms of Requests during core hours Includes: Voice Mail, Email, Web, Fax, Written)	10 Minutes	20 Minutes	20 Minutes	20 Minutes
Percent of problems closed or isolated during the initial call to the help desk support center. The number of Tier 1 Trouble Tickets that are resolved to the users satisfaction and closed without further contract with the customer. This include questions concerning supported software, hardware, and the DCE. Tickets reopened by the customer citing the same problem will not count as closed on the first contract.	80%	80%	80%	80%
Add, Change, Delete User Account The total time from receiving the request to add, change or delete a user account until the ticket is closed. Includes the time necessary to receive all required NRC authorizations, complete required documentation, and notifying customer of completed action.	15 minutes	1 hour	1 hour	4 hours
Security Profile Maintenance Create, amend, or delete a User's access rights to applications.	15 minutes	1 hour	1 hour	4 hours
Update/Reset Password Respond	15 minutes	15 minutes	15 minutes	1 hour
Update/Reset Password Resolve	15 minutes	1 hour	1 hour	2 hours
Restore Files Respond (Restore To Desktop)	1 hour	2 hours	2 hours	User Duty
Restore Files Resolve (Restore To Desktop)	2 hours	4 hours	4 hours	User Duty
Reports Services				
Performance Analysis Report (Summary report showing capacity statistics and trends and recommendations for improvement)	Monthly	Monthly	Monthly	Monthly
Report Distribution	E-mail, Intranet, Fax	E-mail, Intranet, Fax	E-mail, Intranet, Fax	E-mail, Intranet, Fax
Resolution of Unanswered calls	call goes to voice mail for call back	call goes to voice mail for call back	call goes to voice mail for call back	call goes to voice mail for call back
Outside Primary Support Period Help Desk Services				
Outside Primary Support Hours (Local Customer Time)	6pm - 6am	6pm - 6am	6pm - 6am	6pm - 6am
Number of calls or Incident Responses. (In calls per desktop component per month. The total number of calls will be based on the aggregate of all desktop components, rounded to the nearest whole number.)	0.4	0.2	0.1	None
Time To Answer Call or Callback	Start of next business day	Start of next business day	Start of next business day	Start of next business day
Percent of calls answered or called back within the required time.	90%	90%	90%	80%

Co ervice Bands General Purpose Desktop Environn				
Service Measurements	**VIP**	**Professional**	**RISE**	**Other (Remote, etc.)**
	CSBGPDT1	**CSBGPDT2**	**CSBGPDT3**	**CSBGPDT4**
The number of calls answered or returned by a person within the specified time divided by the total number of calls received in the support center.				
MAINTENANCE SERVICES (C.3.4)				
Primary Service Period Maintenance Services				
Incident Response Time Time after initial call to the Help Desk or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken. Response can be a phone call to the customer to set up an appointment. Voice Mail notification is acceptable. Response by Email is acceptable	20 minutes	2 Hours	2 Hours	Remote/Mobile 10m
Time to Repair Hardware/Software Problems (After technician responds) The average time during a performance period that it takes to resolve maintenance break/fix problems. The time is measured from technician response to problem resolution. Maintenance includes fixing failures, resolving problems, or completing special diagnostic requests.	1 Hour	4 Hours	4 Hours	4 Hours
Outside Primary Support Period - Maintenance Services				
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.) Note: When responses initiated outside the Primary Support Period overlap the beginning of the Primary Support Period, response times for the Primary Support Period take precedence if they produce an earlier response. Response can be a phone call to the customer to set up an appointment. Voice Mail notification is acceptable. Response by Email is acceptable	Start of next business day	Start of next business day	Start of next business day	Start of next business day
Time to Repair Hardware/Software Problems (After technician responds) The average time during a performance period that it takes to resolve maintenance break/fix problems. The time is measured from technician response to problem resolution. Maintenance includes fixing failures, resolving problems, or completing special diagnostic requests.	2 Hours for designated VIP	N/A	N/A	N/A
Satisfaction Survey				
Trouble Ticket Follow-up	Daily	Weekly	Weekly	Weekly

Co rvice Bands General Purpose Desktop Environn				
Service Measurements	**VIP**	**Professional**	**RISE**	**Other (Remote, etc.)**
	CSBGPDT1	**CSBGPDT2**	**CSBGPDT3**	**CSBGPDT4**
Follow-up survey with customers for whom a trouble ticket has been established.				
Customer Survey Surveys conducted for the entire NRC user population,	Semi-annually	Semi-annually	Semi-annually	Annually
Customer Survey Rating Average customer service rating based on a 5 point scale, where 5 is the highest rating. (Contractor may recommend a different scale)	90% of survey response is 4.5 or Higher	90% of survey response is 4.5 or Higher	90% of survey response is 4.5 or Higher	90% of survey response is 4.5 or Higher
Reports Services				
Call Analysis Reports (Reports detailing and summarizing all measurable performance information for assets and support, e.g., call volumes, problem statistics, call and problem resolution statistics, asset status, and technology statistics.)	Monthly	Monthly	Monthly	Monthly
Incident Exception Reports – (Incident reporting for services not completed within stated time frames)	Weekly Summary	Weekly Summary	Weekly Summary	Weekly Summary
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Asset Management Service Area (C.3.2)				
General Services				
Technology Refreshment Rate The period of time from the original component installation through the user acceptance of the replacement component. Individual instances of retaining components beyond the AQL must be approved by the NRC and will not be counted for incentive or disincentive.	36 Months	36 Months	36 Months	36 Months
Technology Refreshment Deployment Time Time to install component following agreement to install	5 Days	5 Days	5 Days	5 Days
Days To Remove Existing Asset (Component Removal) Includes collection, data wipe, itemizations of components that are removed, due to obsolescence, refreshment, or replacement, in preparation for disposal or reissue.	15 Days	15 Days	15 Days	15 Days
Automated Inventory Management Tracks component location, service information, asset number Accessible by NRC	Yes	Yes	Yes	Yes
Acquisition of Special Request Property Includes updating of NRC Property Management System to reflect NRC property accountability.	As Scheduled	As Scheduled	As Scheduled	As Scheduled
COTS Software Deployment	As Scheduled	As Scheduled	As Scheduled	As Scheduled
Reports Services				
Technology Management Reports Reports detailing and summarizing technology status and requirements, market trends,	Semi-Annually Jan / Jul)	Semi-Annually Jan / Jul)	Semi-Annually (Jan/Jul)	Semi-Annually (Jan/Jul)

Cc ervice Bands General Purpose Desktop Environ				
Service Measurements	VIP	Professional	RISE	Other (Remote, etc.)
	CSBGPDT1	CSBGPDT2	CSBGPDT3	CSBGPDT4
and recommended action				
Report Distribution	E-mail, Intranet, Fax	E-mail, Intranet, Fax	E-mail, Intranet, Fax	E-mail, Intranet, Fax

Development & Integration Service Bands	
Service Measurements	**NRC**
DEVELOPMENT & INTEGRATION (C.3.5)	
Timeliness (Compliance with Development and Integrations Schedules) Measured by successfully completing project milestones and schedules as agreed to	As Scheduled
Quality Measured by number and/or impact scope of an unsuccessful upgrade	A min. of 90% for initial pilots A min. of 95% for secondary pilots A min of 98.5% for production implementation
Primary Service Period for Consolidated Test Facility All systems must be configured as required for testing	As Scheduled
Consolidated Test Facility: Time to restore Baseline	4 Hours
CTF Capacity (number of supported test environments)	min. 5 concurrent
CTF schedule	on-line, web based
CTF Standard Regression Testing Matrix	on-line, web based
Reports Services	
Technology Management Reports Reports detailing and summarizing future infrastructure requirements, upgrade strategies, stakeholder requirements, market trends, and recommended action.	Semi-Annually (Jan / Jul)
Project Schedule Reports	Weekly
Release Forecast Schedule Reports	Weekly
Long Range Release Forecast Schedule Reports	Quarterly
Report Distribution	E-mail, Intranet

e Service Bands Scientific and Engineering Des. Environment		
Service Measurements	**High Performance**	**Test/Development**
	CSBSEDT2	**CSBSEDT4**
Infrastructure Management Service Area (C.3.1)		
General Services		
Availability during the primary support period. (Number of hours of service availability divided by the number of hours in the primary support period, per month)	97%	93%
File, Print, Application Server Availability The average percentage of time each network server is fully available to the users. The percentage is calculated by dividing the sum of down times (hours down times the number of users affected) by the Total Hours of availability times the total number of users, minus the sum of the scheduled outages (the downtime of the outage times the number of affected users. See the note bellow for further detail	99.6%	99.6%
Network Throughput Throughput is the rate at which data is transferred through the network, expressed in Megabits per second (MBPS), and measured by counting the bytes transported during a specified period of time.	> 10 Mbps of data to the desktop	> 10 Mbps of data to the desktop
Network Bandwidth		
Scalability		
File Server Storage Volume The amount of space, measured in Megabytes (MB) available to each user in a network file server.	100MB per user	50MB per user
Electronic Performance Monitoring, Incident Detection, and Diagnostic Service (Provides automated incident or fault detection and response initiation. Applies to components which are powered up, operating, and network connected.)	Yes	Yes
Electronic Notification Service (Components which are powered up, operating, and network connected)	Yes	Yes
Electronic Software Distribution (Components which are powered up, operating, and network connected)	Yes	Yes
Electronic Topology/Configuration Management Includes Configuration Management for all DCE components: Current description of image, current configuration of hardware and software, current location Accessible by NRC	Yes	Yes
Performance Analysis and Tuning (Components which are powered up, operating, and network connected)	Monthly	Upon Request (Limit 4 per year)
Virus Scanning	Yes	Yes
Network File Backup		

...re Service Bands Scientific and Engineering De... Environment		
Service Measurements	**High Performance**	**Test/Development**
	CSBSEDT2	**CSBSEDT4**
Local Drive Storage Backup To Network Data files in Standardized Directory only for components that are powered up, operating, and connected to the network.	Weekly	None, User Duty
User Administration Services		
HELP DESK (C.3.3)		
General Services		
Primary Support Period (Hours x Days)	12x5	12x5
Primary Support Days	Mon. - Fri.	Mon. - Fri.
Primary Support Hours (Local Customer Time)	6am - 6pm	6am - 6pm
Number of Calls or Incident Responses Included in Service During Primary Support Period.	Unlimited	Unlimited
Time To Answer Calls The time from when the customer make the last ACD selection (if required) until the call is answered by a live person. (Can't identify a VIP at this time)	15 Seconds	15 Seconds
Percentage of Calls Answered Within Stated Time From First Ring	90%	70%
Number of rings before Voice Mail responds during core hours	4	5
Percentage of calls going to Voice Mail during Core Hours (Time to Answer Calls)	4%	6%
Percentage of Abandoned Calls	3%	3%
Time to Respond to Other forms of Requests during core hours Includes: Voice Mail, Email, Web, Fax, Written)	20 Minutes	20 Minutes
Percent of problems closed or isolated during the initial call to the help desk support center. The number of Tier 1 Trouble Tickets that are resolved to the users satisfaction and closed without further contract with the customer. This include questions concerning supported software, hardware, and the DCE. Tickets reopened by the customer citing the same problem will not count as closed on the first contract.	80%	80%
Add, Change, Delete User Account The total time from receiving the request to add, change or delete a user account until the ticket is closed. Includes the time necessary to receive all required NRC authorizations, complete required documentation, and notifying customer of completed action.	1 hour	4 hours
Update/Reset Password Respond	15 minutes	2 hours
Update/Reset Password Resolve	1 hour	2 hours
Restore Files Respond (Restore To Desktop)	2 hours	User Duty
Restore Files Resolve (Restore To Desktop)	8 hours	User Duty

e Service Bands Scientific and Engineering Des Environment		
Service Measurements	**High Performance**	**Test/Development**
	CSBSEDT2	**CSBSEDT4**
Reports Services		
Performance Analysis Report (Summary report showing capacity statistics and trends and recommendations for improvement)	Monthly	Monthly
Report Distribution	E-mail, Intranet, Fax	E-mail, Intranet, Fax
Resolution of Unanswered calls	call goes to voice mail for call back	call goes to voice mail for call back
Outside Primary Support Period Help Desk Services		
Outside Primary Support Hours (Local Customer Time)	6pm - 6am	6pm - 6am
Number of calls or Incident Responses. (In calls per desktop component per month. The total number of calls will be based on the aggregate of all desktop components, rounded to the nearest whole number.)	0.2	None
Time To Answer Call or Callback	Start of next business day	Start of next business day
Percent of calls answered or called back within the required time. The number of calls answered or returned by a person within the specified time divided by the total number of calls received in the support center.	90%	90%
MAINTENANCE SERVICES (C.3.4)		
Primary Service Period Maintenance Services		
Incident Response Time Time after initial call to the Help Desk or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken. Response can be a phone call to the customer to set up an appointment. Voice Mail notification is acceptable. Response by Email is acceptable	2 Hours	2 Hours
Time to Repair Hardware/Software Problems (After technician responds) The average time during a performance period that it takes to resolve maintenance break/fix problems. The time is measured from technician response to problem resolution. Maintenance includes fixing failures, resolving problems, or completing special diagnostic requests.	4 Hours	4 Hours
Outside Primary Support Period - Maintenance Services		
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.) Note: When responses initiated outside the Primary Support Period overlap the beginning of the Primary Support Period, response times for the Primary Support Period take precedence if they produce an earlier response. Response can be a phone call to the customer to set up an appointment.	Start of next business day	Start of next business day

ore Service Bands Scientific and Engineering De Environment		
Service Measurements	**High Performance**	**Test/Development**
	CSBSEDT2	**CSBSEDT4**
Voice Mail notification is acceptable. Response by Email is acceptable		
Time to Repair Hardware/Software Problems (After technician responds) The average time during a performance period that it takes to resolve maintenance break/fix problems. The time is measured from technician response to problem resolution. Maintenance includes fixing failures, resolving problems, or completing special diagnostic requests.	N/A	N/A
Satisfaction Survey		
Trouble Ticket Follow-up Follow-up survey with customers for whom a trouble ticket has been established.	Weekly	Weekly
Customer Survey Surveys conducted for the entire NRC user population,	Semi-annually	Semi-Annually
Customer Survey Rating Average customer service rating based on a 5 point scale, where 5 is the highest rating. (Contractor may recommend a different scale)	90% of survey response is 4.5 or Higher	90% of survey response is 4.5 or Higher
Reports Services		
Call Analysis Reports (Reports detailing and summarizing all measurable performance information for assets and support, e.g., call volumes, problem statistics, call and problem resolution statistics, asset status, and technology statistics.)	Monthly	Monthly
Incident Exception Reports – (Incident reporting for services not completed within stated time frames)	Weekly Summary	Weekly Summary
Report Distribution	E-mail, Intranet	E-mail, Intranet
Asset Management Service Area (C.3.2)		
General Services		
Technology Refreshment Rate The period of time from the original component installation through the user acceptance of the replacement component. Individual instances of retaining components beyond the AQL must be approved by the NRC and will not be counted for incentive or disincentive.	36 Months	36 Months
Technology Refreshment Deployment Time Time to install component following agreement to install	5 Days	5 Days
Days To Remove Existing Asset (Component Removal) Includes collection, data wipe, itemizations of components that are removed, due to obsolescence, refreshment, or replacement, in preparation for disposal or reissue.	15 Days	15 Days
Automated Inventory Management Tracks component location, service information, asset number	Yes	Yes

e Service Bands Scientific and Engineering Des Environment		
Service Measurements	**High Performance**	**Test/Development**
	CSBSEDT2	**CSBSEDT4**
Accessible by NRC		
Acquisition of Special Request Property Includes updating of NRC Property Management System to reflect NRC property accountability.	As Scheduled	As Scheduled
COTS Software Deployment	As Scheduled	As Scheduled
Reports Services		
Technology Management Reports Reports detailing and summarizing technology status and requirements, market trends, and recommended action	Semi-Annually (Jan / Jul)	Semi-Annually (Jan/Jul)
Report Distribution	E-mail, Intranet	E-mail, Intranet
DEVELOPMENT & INTEGRATION (C.3.5)		
Primary Service Period for Consolidated Test Facility All systems must be configured as required for testing	As Scheduled	As Scheduled
Consolidated Test Facility: Time to restore Baseline	4 Hours	4 Hours
Reports Services		
Technology Management Reports Reports detailing and summarizing future infrastructure requirements, upgrade strategies, stakeholder requirements, market trends, and recommended action.	Semi-Annually (Jan / Jul)	Semi-Annually (Jan/Jul)
Report Distribution	E-mail, Intranet	E-mail, Intranet
Compliance with Development and Integrations Schedules	As Scheduled	As Scheduled

C Service Bands Portable Desktop Environment				
Service Measurements	**Portable VIP**	**Portable Professional**	**Portable (Travel only)**	**Other**
	CSBPDT1	**CSBPDT2**	**CSBPDT3**	**CSBPDT4**
Infrastructure Management Service Area (C.3.1)				
General Services				
Availability during the primary support period. (Number of hours of service availability divided by the number of hours in the primary support period, per month)	99%	97%	95%	93%
File, Print, Application Server Availability The average percentage of time each network server is fully available to the users. The percentage is calculated by dividing the sum of down times (hours down times the number of users affected) by the Total Hours of availability times the total number of users, minus the sum of the scheduled outages (the downtime of the outage times the number of affected users. See the note bellow for further detail	99.6%	99.6%	99.6%	99.6%
Network Throughput Throughput is the rate at which data is transferred through the network, expressed in Megabits per second (MBPS), and measured by counting the bytes transported during a specified period of time.	> 10 Mbps of data to the desktop	> 10 Mbps of data to the desktop	N/A	N/A
Network Bandwidth				
Scalability				
File Server Storage Volume The amount of space, measured in Megabytes (MB) available to each user in a network file server.	100MB per user	100MB per user	100MB per user	50MB per user
Electronic Performance Monitoring, Incident Detection, and Diagnostic Service (Provides automated incident or fault detection and response initiation. Applies to components which are powered up, operating, and network connected.)	Yes	Yes	Yes	Yes
Electronic Notification Service (Components which are powered up, operating, and network connected)	Yes	Yes	Yes	Yes
Electronic Software Distribution (Components which are powered up, operating, and network connected)	Yes	Yes	Yes	Yes
Electronic Topology/Configuration Management Includes Configuration Management for all DCE components: Current description of image, current configuration of hardware and software, current location Accessible by NRC	Yes	Yes	Yes	Yes
Performance Analysis and Tuning (Components which are powered up, operating, and network connected)	Monthly	Monthly	Upon Request (Limit 4 per year)	Upon Request (Limit 4 per year)
Virus Scanning	Yes	Yes	Yes	Yes

C Service Bands Portable Desktop Environment				
Service Measurements	**Portable VIP**	**Portable Professional**	**Portable (Travel only)**	**Other**
	CSBPDT1	**CSBPDT2**	**CSBPDT3**	**CSBPDT4**
Network File Backup				
Local Drive Storage Backup To Network Data files in Standardized Directory only for components that are powered up, operating, and connected to the network.	None, User Duty	None, User Duty	None, User Duty	None, User Duty
User Administration Services				
HELP DESK (C.3.3)				
General Services				
Primary Support Period (Hours x Days)	12x5	12x5	12x5	12x5
Primary Support Days	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.
Primary Support Hours (Local Customer Time)	6am - 6pm	6am - 6pm	6am - 6pm	6am - 6pm
Number of Calls or Incident Responses Included in Service During Primary Support Period.	Unlimited	Unlimited	Unlimited	Unlimited
Time To Answer Calls The time from when the customer make the last ACD selection (if required) until the call is answered by a live person. (Can't identify a VIP at this time)	15 Seconds	15 Seconds	15 Seconds	15 Seconds
Percentage of Calls Answered Within Stated Time From First Ring	90%	90%	80%	70%
Number of rings before Voice Mail responds during core hours	3	4	4	5
Percentage of calls going to Voice Mail during Core Hours (Time to Answer Calls)	4%	4%	4%	6%
Percentage of Abandoned Calls	3%	3%	3%	3%
Time to Respond to Other forms of Requests during core hours Includes: Voice Mail, Email, Web, Fax, Written)	10 Minutes	20 Minutes	20 Minutes	20 Minutes
Percent of problems closed or isolated during the initial call to the help desk support center. The number of Tier 1 Trouble Tickets that are resolved to the users satisfaction and closed without further contract with the customer. This include questions concerning supported software, hardware, and the DCE. Tickets reopened by the customer citing the same problem will not count as closed on the first contract.	80%	80%	80%	80%
Add, Change, Delete User Account The total time from receiving the request to add, change or delete a user account until the ticket is closed. Includes the time necessary to receive all required NRC authorizations, complete required documentation, and notifying customer of completed action.	15 minutes	1 hour	4 hours	8 hours

C Service Bands Portable Desktop Environment				
Service Measurements	**Portable VIP**	**Portable Professional**	**Portable (Travel only)**	**Other**
	CSBPDT1	**CSBPDT2**	**CSBPDT3**	**CSBPDT4**
Update/Reset Password Respond	15 minutes	15 minutes	15 minutes	2 hours
Update/Reset Password Resolve	15 minutes	1 hour	1 hour	2 hours
Restore Files Respond (Restore To Desktop)	1 hour	2 hours	User Duty	User Duty
Restore Files Resolve (Restore To Desktop)	2 hours	8 hours	User Duty	User Duty
Reports Services				
Performance Analysis Report (Summary report showing capacity statistics and trends and recommendations for improvement)	Monthly	Monthly	Monthly	Quarterly
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Resolution of Unanswered calls	call goes to voice mail for call back	call goes to voice mail for call back	call goes to voice mail for call back	call goes to voice mail for call back
Outside Primary Support Period Help Desk Services				
Outside Primary Support Hours (Local Customer Time)	6pm - 6am	6pm - 6am	6pm - 6am	6pm - 6am
Number of calls or Incident Responses. (In calls per desktop component per month. The total number of calls will be based on the aggregate of all desktop components, rounded to the nearest whole number.)	0.4	0.2	0.1	None
Time To Answer Call or Callback	Start of next business day	Start of next business day	Start of next business day	Start of next business day
Percent of calls answered or called back within the required time. The number of calls answered or returned by a person within the specified time divided by the total number of calls received in the support center.	90%	90%	90%	80%
MAINTENANCE SERVICES (C.3.4)				
Primary Service Period Maintenance Services				
Incident Response Time Time after initial call to the Help Desk or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken. Response can be a phone call to the customer to set up an appointment. Voice Mail notification is acceptable. Response by Email is acceptable	20 minutes	1 Hour	I Hour	Remote/Mobile 10m

C Service Bands Portable Desktop Environment				
Service Measurements	**Portable VIP**	**Portable Professional**	**Portable (Travel only)**	**Other**
	CSBPDT1	**CSBPDT2**	**CSBPDT3**	**CSBPDT4**
Time to Repair Hardware/Software Problems (After technician responds) The average time during a performance period that it takes to resolve maintenance break/fix problems. The time is measured from technician response to problem resolution. Maintenance includes fixing failures, resolving problems, or completing special diagnostic requests. When asset is in remote use and cannot be brought in to the client facility, response and repair times commence when asset is delivered by the user to a local authorized support center. The user will be responsible for picking up the repaired asset from the local authorized support center.	30 minutes	2 Hours	1 Hour (onsite only)	1 Hour
Outside Primary Support Period - Maintenance Services				
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.) Note: When responses initiated outside the Primary Support Period overlap the beginning of the Primary Support Period, response times for the Primary Support Period take precedence if they produce an earlier response. Response can be a phone call to the customer to set up an appointment. Voice Mail notification is acceptable. Response by Email is acceptable	Start of next business day	Start of next business day	Start of next business day	Start of next business day
Time to Repair Hardware/Software Problems (After technician responds) The average time during a performance period that it takes to resolve maintenance break/fix problems. The time is measured from technician response to problem resolution. Maintenance includes fixing failures, resolving problems, or completing special diagnostic requests. When asset is in remote use and cannot be brought in to the client facility, response and repair times commence when asset is delivered by the user to a local authorized support center. The user will be responsible for picking up the repaired asset from the local authorized support center.	N/A	N/A	N/A	N/A
Satisfaction Survey				

C Service Bands Portable Desktop Environment				
Service Measurements	**Portable VIP**	**Portable Professional**	**Portable (Travel only)**	**Other**
	CSBPDT1	**CSBPDT2**	**CSBPDT3**	**CSBPDT4**
Trouble Ticket Follow-up Follow-up survey with customers for whom a trouble ticket has been established.	Daily	Weekly	Weekly	Monthly
Customer Survey Surveys conducted for the entire NRC user population,	Semi-annually	Semi-annually	Semi-annually	Annually
Customer Survey Rating Average customer service rating based on a 5 point scale, where 5 is the highest rating. (Contractor may recommend a different scale)	90% of survey response is 4.5 or Higher	90% of survey response is 4.5 or Higher	90% of survey response is 4.5 or Higher	90% of survey response is 4.5 or Higher
Reports Services				
Call Analysis Reports (Reports detailing and summarizing all measurable performance information for assets and support, e.g., call volumes, problem statistics, call and problem resolution statistics, asset status, and technology statistics.)	Monthly	Monthly	Monthly	Quarterly
Incident Exception Reports – (Incident reporting for services not completed within stated time frames)	Weekly Summary	Weekly Summary	Weekly Summary	Weekly Summary
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Asset Management Service Area (C.3.2)				
General Services				
Technology Refreshment Rate The period of time from the original component installation through the user acceptance of the replacement component. Individual instances of retaining components beyond the AQL must be approved by the NRC and will not be counted for incentive or disincentive.	36 Months	36 Months	36 Months	36 Months
Technology Refreshment Deployment Time Time to install component following agreement to install	5 Days	5 Days	5 Days	5 Days
Days To Remove Existing Asset (Component Removal) Includes collection, data wipe, itemizations of components that are removed, due to obsolescence, refreshment, or replacement, in preparation for disposal or reissue.	15 Days	15 Days	15 Days	15 Days
Automated Inventory Management Tracks component location, service information, asset number Accessible by NRC	Yes	Yes	Yes	Yes
Acquisition of Special Request Property	As Scheduled	As Scheduled	As Scheduled	As Scheduled

C Service Bands Portable Desktop Environment				
Service Measurements	**Portable VIP**	**Portable Professional**	**Portable (Travel only)**	**Other**
	CSBPDT1	**CSBPDT2**	**CSBPDT3**	**CSBPDT4**
Includes updating of NRC Property Management System to reflect NRC property accountability.				
COTS Software Deployment	As Scheduled	As Scheduled	As Scheduled	As Scheduled
Reports Services				
Technology Management Reports Reports detailing and summarizing technology status and requirements, market trends, and recommended action	Semi-Annually (Jan / Jul)	Semi-Annually Jan / Jul)	Semi-Annually (Jan/Jul)	Annually (Jan)
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
DEVELOPMENT & INTEGRATION (C.3.5)				
Primary Service Period for Consolidated Test Facility All systems must be configured as required for testing	As Scheduled	As Scheduled	As Scheduled	As Scheduled
Consolidated Test Facility: Time to restore Baseline	4 Hours	4 Hours	4 Hours	4 Hours
Reports Services				
Technology Management Reports Reports detailing and summarizing future infrastructure requirements, upgrade strategies, stakeholder requirements, market trends, and recommended action.	Semi-Annually (Jan / Jul)	Semi-Annually Jan / Jul)	Semi-Annually (Jan/Jul)	Annually (Jan)
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Compliance with Development and Integrations Schedules	As Scheduled	As Scheduled	As Scheduled	As Scheduled

C[illegible]ervice Band General Purpose Enterprise Server Envir[illegible]nt			
Service Measurements	**Core**	**Option**	**Option**
	CSBGPES1	**CSBGPES2**	**CSBGPES3**
Infrastructure Management Service Area (C.3.1)			
General Services			
Availability during the primary support period. (Number of hours of service availability divided by the number of hours in the primary support period, per month)	99.60%	98.00%	98.00%
File, Print, Application Server Availability The average percentage of time each network server is fully available to the users. The percentage is calculated by dividing the sum of down times (hours down times the number of users affected) by the Total Hours of availability times the total number of users, minus the sum of the scheduled outages (the downtime of the outage times the number of affected users. See the note bellow for further detail	99.6%	99.6%	99.6%
Network Throughput Throughput is the rate at which data is transferred through the network, expressed in Megabits per second (MBPS), and measured by counting the bytes transported during a specified period of time.	> 10 Mbps of data to the desktop	> 10 Mbps of data to the desktop	> 10 Mbps of data to the desktop
Network Bandwidth			
Scalability			
File Server Storage Volume The amount of space, measured in Megabytes (MB) available to each user in a network file server.	100MB per user	100MB per user	N/A
Electronic Performance Monitoring, Incident Detection, and Diagnostic Service (Provides automated incident or fault detection and response initiation. Applies to components which are powered up, operating, and network connected.)	Yes	Yes	Yes
Electronic Notification Service (Components which are powered up, operating, and network connected)	Yes	Yes	Yes
Electronic Software Distribution (Components which are powered up, operating, and network connected)	Yes	Yes	Yes
Electronic Topology/Configuration Management Includes Configuration Management for all DCE components: Current description of image, current configuration of hardware and software, current location Accessible by NRC	Yes	Yes	Yes
Performance Analysis and Tuning (Components which are powered up, operating, and network connected)	Monthly	Monthly	Upon Request (Limit 4 per year)
Virus Scanning	Yes	Yes	Yes
Shared Network Storage Data File Backup	Daily Incremental	Daily Incremental	Daily Incremental
Disaster Recovery Shared Network Storage Data File Backup	Biweekly	Biweekly	Biweekly
User Administration Services			

C... ervice Band General Purpose Enterprise Server Envir... nt			
Service Measurements	**Core**	**Option**	**Option**
	CSBGPES1	**CSBGPES2**	**CSBGPES3**
Restore Files Respond (Restore To Network)	15 minutes	1 hour	2 hours
Restore Files Resolve (Restore To Network)	1 hour	2 hours	4 hours
Report Services			
Performance Analysis Report (Summary report showing capacity statistics and trends and recommendations for improvement)	Monthly	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
User Support Service Area (C.3.3, C.3.4)			
General Services			
Primary Support Period (Hours x Days) See Note 1	12x5	12x5	12x5
Primary Support Days	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.
Primary Support Hours (Local Customer Time)	6am - 6pm	6am - 6pm	6am - 6pm
Help Desk Services			
Help Desk Calls Will Originate From The Desktop	See Desktop	See Desktop	See Desktop
Primary Support Period Maintenance			
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.)	1/2 Hour	2 Hours	4 Hours
Time to Repair Software Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Time to Repair Hardware Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Outside Primary Support Period Maintenance (See Note 3)			
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.) Note: When responses initiated outside the Primary Support Period overlap the beginning of the Primary Support Period, response times for the Primary Support Period take precedence if they produce an earlier response.	4 Hours	6 Hours	Start of Next Business Day
Time to Repair Hardware/Software Problems (After technician responds) The average time during a performance period that it takes to resolve maintenance break/fix problems. The time is measured from technician response to problem resolution. Maintenance includes fixing failures, resolving problems, or completing special diagnostic requests.	2 hours	4 Hours	6 Hours
Reports Services			
Call Analysis Report (Reports detailing and summarizing all measurable performance information for assets and support, e.g., call volumes, problem statistics, call and problem	Monthly	Monthly	Quarterly

C[illegible]ervice Band General Purpose Enterprise Server Envi[illegible]ent			
Service Measurements	**Core**	**Option**	**Option**
	CSBGPES1	**CSBGPES2**	**CSBGPES3**
resolution statistics, asset status, and technology statistics.)			
Incident Exception Reports – (Incident reporting for services not completed within stated time frames)	Weekly Summary	Weekly Summary	Weekly Summary
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Asset Management Service Area (C.3.2)			
General Services			
Technology Refreshment Rate - (Frequency of component replacement with newer technology, from date of initial component installation) See Note 2	36 Months	36 Months	36 Months
Technology Refreshment Deployment Time - (Time to install component following agreement to install.)	30 Days	30 Days	30 Days
Days To Remove Existing Asset	15 Days	15 Days	15 Days
Automated Inventory Management	Yes	Yes	Yes
Report Services			
Technology Management Reports (Reports detailing and summarizing technology status and requirements, market trends, and recommended action.)	Semi-Annually Jan/Jul	Semi-Annually Jan/Jul	Annually Jan
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet

Core S e Band Scientific and Engineering Enterprise Server I onment

Service Measurements	Core	Option	Option
	CSBSEES1	CSBSEES2	CSBSEES3
Infrastructure Management Service Area (C.3.1)			
General Services			
Availability of LAN Architecture/Communications Device/Server Environment during the primary support period. (Number of hours of service availability divided by the number of hours in the primary support period, per month).	99.60%	98.00%	98.00%
Electronic Performance Monitoring, Incident Detection, and Diagnostic Service (Provides automated incident or fault detection and response initiation. Applies to components which are powered up, operating, and network connected.)	Yes	Yes	Yes
Electronic Notification Service (Components which are powered up, operating, and network connected)	Yes	Yes	Yes
Electronic Software Distribution (Components which are powered up, operating, and network connected)	Yes	Yes	Yes
Electronic Topology/Configuration Management	Yes	Yes	Yes
Virus Scanning	Yes	Yes	Yes
Shared Network Storage Data File Backup	Daily Incremental	Daily Incremental	Daily Incremental
Disaster Recovery Shared Network Storage Data File Backup	Biweekly	Biweekly	Biweekly
User Administration Services			
Restore Files Respond (Restore To Network)	15 minutes	1 hour	2 hours
Restore Files Resolve (Restore To Network)	1 hour	2 hours	4 hours
Report Services			
Performance Analysis Report (Summary report showing capacity statistics and trends and recommendations for improvement)	Monthly	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
User Support Service Area (C.3.3, C.3.4)			
General Services			
Primary Support Period (Hours x Days) See Note 1	12x5	12x5	12x5
Primary Support Days	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.
Primary Support Hours (Local Customer Time)	6am - 6pm	6am - 6pm	6am - 6pm
Help Desk Services			
Help Desk Calls Will Originate From The Desktop	See Desktop	See Desktop	See Desktop
Primary Support Period Maintenance			

Core S[illegible]e Band Scientific and Engineering Enterprise Server E[illegible]onment			
Service Measurements	**Core**	**Option**	**Option**
	CSBSEES1	**CSBSEES2**	**CSBSEES3**
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.)	1/2 Half Hour	2 Hours	4 Hours
Time to Repair Software Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Time to Repair Hardware Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Outside Primary Support Period Maintenance (See Note 3)			
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.) Note: When responses initiated outside the Primary Support Period overlap the beginning of the Primary Support Period, response times for the Primary Support Period take precedence if they produce an earlier response.	4 Hours	6 Hours	Start of Next Business Day
Time to Repair Software Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Time to Repair Hardware Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Reports Services			
Call Analysis Report (Reports detailing and summarizing all measurable performance information for assets and support, e.g., call volumes, problem statistics, call and problem resolution statistics, asset status, and technology statistics.)	Monthly	Monthly	Quarterly
Incident Exception Reports (Incident reporting for services not completed within stated time frames)	Weekly Summary	Weekly Summary	Weekly Summary
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Asset Management Service Area (C.3.2)			
General Services			
Technology Refreshment Rate - (Frequency of component replacement with newer technology, from date of initial component installation) See Note 2	36 Months	36 Months	36 Months
Technology Refreshment Deployment Time - (Time to install component following agreement to install.)	30 days	30 days	30 days
Days To Remove Existing Asset	15 Days	15 Days	15 Days
Automated Inventory Management	Yes	Yes	Yes
Report Services			
Technology Management Reports (Reports detailing and summarizing technology status and requirements, market trends, and recommended action.)	Semi-Annually Jan/Jul	Semi-Annually Jan/Jul	Annually Jan
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet

Service Band Scientific and Engineering LAN Server E onment			
Service Measurements	**Core**	**Option**	**Option**
	CSBSELS1	**CSBSELS2**	**CSBSELS3**
Infrastructure Management Service Area (C.3.1)			
General Services			
Availability of LAN Architecture/Communications Device/Server Environment during the primary support period. (Number of hours of service availability divided by the number of hours in the primary support period, per month).	99.60%	98.00%	98.00%
Electronic Performance Monitoring, Incident Detection, and Diagnostic Service (Provides automated incident or fault detection and response initiation. Applies to components which are powered up, operating, and network connected.)	Yes	Yes	Yes
Electronic Notification Service (Components which are powered up, operating, and network connected)	Yes	Yes	Yes
Electronic Software Distribution (Components which are powered up, operating, and network connected)	Yes	Yes	Yes
Electronic Topology/Configuration Management	Yes	Yes	Yes
Virus Scanning	Yes	Yes	Yes
Shared Network Storage Data File Backup	Daily Incremental	Daily Incremental	Daily Incremental
Disaster Recovery Shared Network Storage Data File Backup	Biweekly	Biweekly	Biweekly
User Administration Services			
Restore Files Respond (Restore To Network)	15 minutes	2 hours	4 hours
Restore Files Resolve (Restore To Network)	2 hours	4 hours	Next Day
Report Services			
Performance Analysis Report (Summary report showing capacity statistics and trends and recommendations for improvement)	Monthly	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
User Support Service Area (C.3.3, C.3.4)			
General Services			
Primary Support Period (Hours x Days) See Note 1	12x5	12x5	12x5
Primary Support Days	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.
Primary Support Hours (Local Customer Time)	6am - 6pm	6am - 6pm	6am - 6pm
Help Desk Services			
Help Desk Calls Will Originate From The Desktop	See Desktop	See Desktop	See Desktop
Primary Support Period Maintenance			

Service Band Scientific and Engineering LAN Server . ronment			
Service Measurements	**Core**	**Option**	**Option**
	CSBSELS1	**CSBSELS2**	**CSBSELS3**
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken..)	1/2 Hour	2 Hours	4 Hours
Time to Repair Software Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Time to Repair Hardware Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Outside Primary Support Period Maintenance (See Note 3)			
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.) Note: When responses initiated outside the Primary Support Period overlap the beginning of the Primary Support Period, response times for the Primary Support Period take precedence if they produce an earlier response.	4 Hours	6 Hours	Start of Next Business Day
Time to Repair Software Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Time to Repair Hardware Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Reports Services			
Call Analysis Report (Reports detailing and summarizing all measurable performance information for assets and support, e.g., call volumes, problem statistics, call and problem resolution statistics, asset status, and technology statistics.)	Monthly	Monthly	Quarterly
Incident Exception Reports – (Incident reporting for services not completed within stated time frames)	Weekly Summary	Weekly Summary	Weekly Summary
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Asset Management Service Area (C.3.2)			
General Services			
Technology Refreshment Rate - (Frequency of component replacement with newer technology, from date of initial component installation) See Note 2	36 Months	36 Months	36 Months
Technology Refreshment Deployment Time - (Time to install component following agreement to install.)	30 Days	30 Days	30 Days
Days To Remove Existing Asset	15 Days	15 Days	15 Days
Automated Inventory Management	Yes	Yes	Yes
Report Services			
Technology Management Reports (Reports detailing and summarizing technology status and requirements, market trends, and recommended action.)	Semi-Annually (Jan/Jul)	Semi-Annually (Jan/Jul)	Annually (Jan)
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet

Core Service Band Network Printer Environment

Service Measurements	Premium	Core HQ/Reg	Option
	CSBNP1	CSBNP2	CSBNP3
Infrastructure Management Service Area (C.3.1)			
General Services			
Availability during the primary support period. (Number of hours of service availability divided by the number of hours in the primary support period, per month).	99%	97%	95%
Electronic Performance Monitoring, Incident Detection, and Diagnostic Service (Provides automated incident or fault detection and response initiation. Applies to components which should normally be powered up, operating, and network connected).	Yes	Yes	Yes
Electronic Notification Service	Yes	Yes	Yes
Report Services			
Performance Analysis Report (Summary report showing capacity statistics and trends and recommendations for improvement).	Monthly	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
User Support Service Area (C.3.3, C.3.4)			
General Services			
Primary Support Period (Hours x Days) See Note 1	12x5	12x5	12x5
Primary Support Days	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.
Primary Support Hours (Local Customer Time)	6am - 6pm	6am - 6pm	6am - 6pm
Help Desk Services			
Help Desk Calls Will Originate From The Desktop	See Desktop	See Desktop	See Desktop
Primary Support Period Maintenance			
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken). If print jobs can be re-routed to another device within the same workgroup, add two (2) hours to the appropriate response time.	One Hour	Two Hours	Four Hours
Time to Repair Software Problems (After technician responds)	Two Hours	Four Hours	Six Hours
Time to Repair Hardware Problems (After technician responds)	Four Hours	Eight Hours	Twelve Hours
Outside Primary Support Period Maintenance (See Note 3)			

Core Service Band Network Printer Environment

Service Measurements	Premium	Core HQ/Reg	Option
	CSBNP1	CSBNP2	CSBNP3
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken). Note: When responses initiated outside the Primary Support Period overlap the beginning of the Primary Support Period, response times for the Primary Support Period take precedence if they produce an earlier response. If print jobs can be re-routed to another device within the same workgroup, add two hours to the appropriate response time.	Two Hours	Four Hours	Six Hours
Reports Services			
Call Analysis Report (Reports detailing and summarizing performance information for assets and support, e.g., call volumes, problem statistics, call and problem resolution statistics, asset status, and technology statistics).	Monthly	Monthly	Quarterly
Incident Exception Reports (Incident reporting for services not completed within stated time frames).	Weekly Summary	Weekly Summary	Weekly Summary
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Asset Management Service Area (C.3.2)			
General Services			
Technology Refreshment Rate (Frequency of component replacement with newer technology, from date of initial component installation). See Note 2	36 Months	36 Months	36 Months
Technology Refreshment Deployment Time (Time to install component following agreement to install.)	30 days	30 days	30 days
Days To Remove Existing Asset	15 Days	15 Days	15 Days
Automated Inventory Management	Yes	Yes	Yes
Report Services			
Technology Management Reports (Reports detailing and summarizing technology status and requirements, market trends, and recommended action).	Semi-Annually	Semi-Annually	Annually
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet

Core Service Band Communications Environment

Service Measurements	Core	Option	Option
Infrastructure Management Service Area (C.3.1)			
General Services			
Availability of LAN Architecture/Communications Device/Server Environment during the primary support period. (Number of hours of service availability divided by the number of hours in the primary support period, per month).	99.60%	98.00%	98.00%
Electronic Performance Monitoring, Incident Detection, and Diagnostic Service (Provides automated incident or fault detection and response initiation. Applies to components which are powered up, operating, and network connected.)	Yes	Yes	Yes
Electronic Notification Service (Components which are powered up, operating, and network connected)	Yes	Yes	Yes
Electronic Software Distribution (Components which are powered up, operating, and network connected)	Yes	Yes	Yes
Electronic Topology/Configuration Management	Yes	Yes	Yes
Report Services			
Performance Analysis Report (Summary report showing capacity statistics and trends and recommendations for improvement)	Monthly	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
User Support Service Area (C.3.3, C.3.4)			
General Services			
Primary Support Period (Hours x Days) See Note 1	12x5	12x5	12x5
Primary Support Days	Mon. - Fri.	Mon. - Fri.	Mon. - Fri.
Primary Support Hours (Local Customer Time)	6am -6pm	6am - 6pm	6am - 6pm
Help Desk Services			
Help Desk Calls Will Originate From The Desktop	See Desktop	See Desktop	See Desktop
Primary Support Period Maintenance			
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.)	1/2 Hour	1 Hours	4 Hours
Time to Repair Software Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Time to Repair Hardware Problems (After technician responds)	4 Hours	8 Hours	12 Hours

Core Service Band Communications Environment

Service Measurements	Core	Option	Option
Outside Primary Support Period Maintenance (See Note 3)			
Incident Response Time (Time after initial call to the support center or the initial incident detection for a technician to respond on-site at the client facility or from a facility with remote operating capability. Remote response requires that the client be contacted within the response time and notified that action is being taken.) Note: When responses initiated outside the Primary Support Period overlap the beginning of the Primary Support Period, response times for the Primary Support Period take precedence if they produce an earlier response.	4 Hours	6 Hours	Start of Next Business Day
Time to Repair Software Problems (After technician responds)	2 Hours	4 Hours	6 Hours
Time to Repair Hardware Problems (After technician responds)	4 Hours	8 Hours	12 Hours
Reports Services			
Call Analysis Report (Reports detailing and summarizing all measurable performance information for assets and support, e.g., call volumes, problem statistics, call and problem resolution statistics, asset status, and technology statistics.)	Monthly	Monthly	Quarterly
Incident Exception Reports – (Incident reporting for services not completed within stated time frames)	Weekly Summary	Weekly Summary	Weekly Summary
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet
Asset Management Service Area (C.3.2)			
Technology Refreshment Rate - (Frequency of component replacement with newer technology, from date of initial component installation) See Note 2	36 Months	36 Months	36 Months
Technology Refreshment Deployment Time - (Time to install component following agreement to install.)	30 Days	30 Days	30 Days
Days To Remove Existing Asset	15 Days	15 Days	15 Days
Automated Inventory Management	Yes	Yes	Yes
Report Services			
Technology Management Reports (Reports detailing and summarizing technology status and requirements, market trends, and recommended action.)	Semi-Annually	Semi-Annually	Annually
Report Distribution	E-mail, Intranet	E-mail, Intranet	E-mail, Intranet

Catalog Services		
Service Measurements	**NRC VIP**	**NRC Professional**
COTS Peripheral/Hardware Catalog (C.3.7.1)		
Electronic Online Catalog	Yes	Yes
Add item to Catalog	5 working days from request	5 working days from request
Delivery, installation, and initial training	3 working days from date of order	5 working days from date of order
Reports Services		
Technology Management Reports Reports detailing and summarizing future infrastructure requirements, upgrade strategies, stakeholder requirements, market trends, new catalog services and recommended action.	Semi-Annually (Jan / Jul)	Semi-Annually (Jan / Jul)
Summary w/ invoice by office	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet
COTS Software Catalog (C.3.7.2)		
Electronic Online Catalog	Yes	Yes
Add item to Catalog	5 working days from request	5 working days from request
Delivery, installation, and initial training	3 working days from date of order	5 working days from date of order
Reports Services		
Technology Management Reports Reports detailing and summarizing future infrastructure requirements, upgrade strategies, stakeholder requirements, market trends, new catalog services and recommended action.	Semi-Annually (Jan / Jul)	Semi-Annually (Jan / Jul)
Summary w/ invoice by office	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet
Services Support Catalog (C.3.7.1)		
Electronic Online Catalog	Yes	Yes
Add item to Catalog	5 working days from request	5 working days from request
Delivery of services	1 working days from date of order	3 working days from date of order
Reports Services		
Technology Management Reports	Semi-Annually	Semi-Annually

Reports ng and summarizing future infrastructure requirements, upgrad tegies, stakeholder requirements, market trends, new catalog services and recommended action.	(Jan / Jul)	(Jan / Jul)
Summary w/ invoice by office	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet
Maintenance Catalog (C.3.7.4)		
Electronic Online Catalog	Yes	Yes
Add item to Catalog	5 working days from request	5 working days from request
Performance of service	2 Hours from order	1 working days from date of order
Reports Services		
Technology Management Reports Reports detailing and summarizing future infrastructure requirements, upgrade strategies, stakeholder requirements, market trends, new catalog services and recommended action.	Semi-Annually (Jan / Jul)	Semi-Annually (Jan / Jul)
Summary w/ invoice by office	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet
Training Catalog (C.3.7.5)		
Electronic Online Catalog	Yes	Yes
Add item to Catalog	5 working days from request	5 working days from request
Performance of service	3 working days from date of order	5 working days from date of order or as scheduled
Reports Services		
Technology Management Reports Reports detailing and summarizing future infrastructure requirements, upgrade strategies, stakeholder requirements, market trends, new catalog services and recommended action.	Semi-Annually (Jan / Jul)	Semi-Annually (Jan / Jul)
Summary w/ invoice by office	Monthly	Monthly
Report Distribution	E-mail, Intranet	E-mail, Intranet

NRC NETWORK PRINTERS

Network Printer	LOCATION	BW/Color	Memory	IPX Name	Hardware Address
Centronics Printer/Plotter	HQ	Color	?	MINCOLOR-O9E6	0060B09AFDC2
Centronics Printer/Plotter	HQ	Color	?	EPSON870-O3E11	0060B02E0EAD
Centronics Printer/Plotter	HQ	Color	?	EPSON870-T2A19	0060B02E0ECE
Centronics Printer/Plotter	HQ	Color	?	AMS_PAYPERS	0060B0319690
Centronics Printer/Plotter	HQ	Color	?	HP560C-O16E21	0060B0FCD72A
HP 2500C	HQ	Color	?	HP2500C-O16D5	1083597034
HP Color LaserJet	HQ	Color	?	HPCOLOR-T6D2	1.08E+09
HP Color LaserJet	HQ	Color	?	HPLCOLOR-T4E23	80009605065
HP Color LaserJet 4500	HQ	Color	?	HPCOLOR4500-T7F7	0010832B36AF
HP Color LaserJet 4500	HQ	Color	?	HP4500DN-T4F38	00108375A376
HP Color LaserJet 4500	HQ	Color	?	HP4500DN-T2F18	00108373CD35
HP Color LaserJet 4500	HQ	Color	?	HP4500-T5E26	0030C18EF5A0
HP Color LaserJet 4500	HQ	Color	?	HPCOLOR4500-T6E58	00108329FCEB
HP Color LaserJet 4500	HQ	Color	?	HP4500DN-O13G3	00108375E3F7
HP Color LaserJet 4500	HQ	Color	?	HP4500DN-T8E1	00108375AB87
HP Color LaserJet 4500	HQ	Color	?	HP4500-T2E10	0010837721EF
HP Color LaserJet 4500	HQ	Color	?	HP4500DN-T7D14	001083F3B6EE
HP Color LaserJet 4500	HQ	Color	?	HPCOLOR4500-T8K2	00108355CB71
HP Color LaserJet 4500	HQ	Color	?	HP4500C-T3F7	0010832B0A5B
HP Color LaserJet 4500	HQ	Color	?	HP4500-O17H19	001083F3C9EA
HP Color LaserJet 4500	HQ	Color	?	HPCOLOR4500-T8D42	001083420AFA
HP Color LaserJet 5	HQ	Color	?	HP5COLOR-T9F11A	0060B0371182
HP Color LaserJet 5M	HQ	Color	?	HP5MCOLOR-O5E5	0060B0ABD22A
HP Color LaserJet 5M	HQ	Color	?	HP5MCOLOR-O18F8	0060B028AE46
HP Color LaserJet 5M	HQ	Color	?	HP5COLOR-NC1	080009AC492B
HP DeskJet 1220C	HQ	Color	?	HP1220C-T4E8	0060B02DA80A
HP DeskJet 1600C	HQ	Color	?	HP1600C-T9D12	0060B0611359
HP DeskJet 1600CM	HQ	B/W	?	HP1600CM-O15D5	0060B0E7FCDD
HP LaserJet 4/4M	HQ	B/W	?	HP4-T6K4	0060B025EBF1
HP LaserJet 4/4M	HQ	B/W	?	HP4-EXEC-1	0060B0D61DF5
HP LaserJet 4050	HQ	B/W	?	SKPHOPEH4050	00108392F482
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T5B9	0060B014EB25
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T2D24	0060B0D62D4C
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-TRN-T3B17A	08000960A7FD
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O3C3	0060B0C7E1E6
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3E19	0060B0CAD53B
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3B17B	0060B0C90E53
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O15H12	0060B0E8D5D3
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T2C1	080009F9CD33
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-TRN-3B21	0060B0E8E5D9
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3E6	0800096050AF
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O16H2	0060B0E5AB84
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T5D27	08000960C0C2
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3B1	0060B0908D81
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O14E17	08000960B72E
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T9E31A	080009E76E60
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T6G1	080009E5A8CD
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T5E30	1.08E+07
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T6D59	0060B0D6836D
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O16E15	0060B03FBDE2
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3F1	08000961A0B8
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T8D34	080009A98E42
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T4A10	0060B0E8D54E
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O16H7	080009D73478
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O13C7	0060B0D6F354
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T2D32	0060B0D62371
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T7E37	0060B0C98256
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T10E51	08000961C070

NRC NETWORK PRINTERS

Network Printer	LOCATION	BW/Color	Memory	IPX Name	Hardware Address
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T9C1	0060B0E8E569
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T7E4	0060B0E8A5DB
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3D45	0060B0D643C2
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T2E3	0800096087BF
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T6E55	08000961E0F5
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T4E8	0060B02DA80A
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O12E5A	08000960A7A6
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3B19B	0060B0AD411D
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SICSC-T4C16	0060B090E36A
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3D4	08000960C0B0
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O15B2	0060B0E7FC43
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O13H6	0060B0D6F36B
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T7E27	0060B0BF06A8
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O16D20	0060B0BF06D3
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T4A2	0060B0C79163
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T6K5	0060B0E5D967
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T7C2	0060B0E8E575
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3D21	80009608731
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3B5	0060B0C650B9
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T10F13	0060B0E8D520
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3F5	0060B0E8C525
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-TRN-T3B21A	0060B0D6F3FB
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T5E19	0800096010B6
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T3B19A	0060B0B9E34E
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-O16H12	080009AA213D
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T9F29	0060B0D623C0
HP LaserJet 4Si/4Si MX	HQ	B/W	18 MB	HP4SI-T2E12	0060B0D6E3CD
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9E4	080009E684F0
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T3C14	80009608722
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8A31	080009AAB960
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O3E23	080009E119DF
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O13D12	1083060934
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6E70	080009AC3E96
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O2H3	080009D7340F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9C24	080009E1F9D1
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O11E26	080009E682B5
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O9D22	080009F7155E
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10H1	080009E61CFF
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O5H6	080009E119DB
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6A1-PS	080009ACFEE7
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O17H5	080009E77E94
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6E30	08000960C0BE
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6F17	0060B0E7FC8D
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O6E7	0060B0E7ECD2
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O17A3	080009D754DC
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8A17	080009E55C96
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T4D4	080009AC0234
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6D20A	0060B07540FC
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7F27	0060B0D623AC
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7F19	080009CC60CA
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10F16	080009D7341B
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9A45	80009608733
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T2F18	080009D8089C
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8D50	0010830609F4
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6E58	080009E66C17
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O10G12	080009E566FC
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O15D2	080009E1F984
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O7A15	0010830609DF

NRC NETWORK PRINTERS

Network Printer	LOCATION	BW/Color	Memory	IPX Name	Hardware Address
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T5D17A	0060B0C92EAF
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O5E15	0800096087A6
HP LaserJet 5Si	HQ	B/W	24 MB	HP4SI-T5D22	0060B0D62391
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10E6	080009E52697
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9D41	080009D82DC5
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O8G16	080009E1F99D
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T4C18	00108307D3EC
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O12H4	080009E682B7
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T3B39	0060B0C7917B
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6D49	080009ACFEE1
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9C4	0060B0D6A378
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8E22	080009E185D9
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O18F8	0060B0CB6B91
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8E1	080009D76453
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T2D1	080009D73452
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O13E11	080009E684EF
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8F19	080009D872E6
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O3E13	080009E6940B
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9D26	080009E1F9A6
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7J9	080009E52693
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6E7	00108307D353
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O2A12	080009E52692
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10E32	080009E185D4
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI_2ND_FLOOR_PS	080009E67C78
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O14G15	080009E5194F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9F3	080009E5ED24
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O15A2	080009E52694
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7A19	080009E77EBF
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O7D2	080009D75462
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O18H15	0800096087B8
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6C34	080009E5826C
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T2C12	080009AA7423
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O5A2	080009D744B6
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8F37	080009D838D2
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T2A4	080009E73EAB
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O17F18	080009AA2147
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9D8	080009D7447B
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O13D13	080009CC7034
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6C20	080009AA21C4
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10E21	080009E67CA4
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O14A3	080009E5DD1E
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O3E3	080009E55C97
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O15E1	080009E67C9D
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8E14	0060B0D63D4F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9A1	080009D76452
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O14H22	0060B0AE01E8
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O3G1	080009E55C95
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O4E15	080009E5E893
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O16D1	080009AA990A
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T3F15	00108307D305
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6D41	080009E65C3D
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7E40	080009E5CD63
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T5E41	80009605067
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O6D17	080009E55CA2
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7D59	080009E55CA6
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O11H25	080009E526A5
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9E57	080009E73E29
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-OP134	080009E73E9D

NRC NETWORK PRINTERS

Network Printer	LOCATION	BW/Color	Memory	IPX Name	Hardware Address
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10D20	080009E75EFE
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9D20	0060B0D663FB
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6E20	080009D70ED7
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9F34	080009E62C07
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8B7	080009D81A38
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T5B9	080009E65CDC
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O18E12	0060B0E5EBD6
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O8E3	080009D754EA
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O9D1	080009E1F977
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O12D20	080009D832BF
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O8F15	080009AA997F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7D27	080009E73EA5
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O17H21	080009E67C63
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O14H4	080009F75572
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10D5	0060B0E8E559
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O6D1A	080009E56C38
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O11A11	080009D82DCB
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O16H21	0800096097C6
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O3C4	080009E119E0
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8C5	0060B037DAA4
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9E30	080009E5269A
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O14F20	080009E0DB3C
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-CSC123	080009D764E1
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O2D18	080009E73E15
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T3B19	080009D72C32
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6E36	0060B0E8D577
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10L7	080009D744E1
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O15H2	080009D77434
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O18G4	0060B0D6232E
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7D33	00108307F3DC
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9B3	080009E119B0
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O16E7	080009E75EFC
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O3D7	080009E185AE
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O12H2	080009D75444
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O14E5A	080009E75ED1
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O13H6	080009E71ED4
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6F7	00108307E344
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6D6	080009D72CF7
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O4E3	080009E5269C
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O1F21	080009E73EC0
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O8H4	080009AAA91F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O17D17	080009D714C8
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10F52	080009CC707F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O10A1	080009E73E7D
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8K9	0060B0ABE492
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O10D5	080009D80843
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6D7	080009D80894
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-NCCS	080009D7449F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10F6	080009E71E8E
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10K7	080009D77429
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O17F5	080009E1894C
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T4F38	08000960505F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T3E4	080009E55CAB
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T5C7	080009D72487
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9K2	080009E66C0D
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7C6	080009D83D7E
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7I1	08000960A7C4
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7I2	080009E62C14

NRC NETWORK PRINTERS

Network Printer	LOCATION	BW/Color	Memory	IPX Name	Hardware Address
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O7D24	080009B6DB4F
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O9H8	080009D7441B
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O6H4	0800096077DF
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8D14	080009E74E56
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O15D5	080009E76E55
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9E47	080009E66C10
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7D22	080009D75481
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O10H6	0060B097E269
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O15H21	080009D734FE
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7J10	080009AAA916
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T6A2	080009AA31D7
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O11E1	0060B0B9EBAB
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T7F3	080009D744D3
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O17D5	080009AAB96A
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T9D2	0060B0D61DDB
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O16E21	080009E73EA1
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O2B2	080009E1C5BD
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T8F3	80009608728
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O17H16	080009E73E2A
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O7A1	0060B0E8A56C
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T10C9	080009E65C90
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O16A4	080009E76E03
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O12E22	080009D7441A
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T2E14	080009E71EA7
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-O2G11	080009F7E6DF
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T3B17	080009E119D2
HP LaserJet 5Si	HQ	B/W	24 MB	HP5SI-T4D28	080009D73418
HP LaserJet 8100	HQ	B/W	?	HP8100-T4F16	0030C18F9040
Centronics Printer/Plotter	RGN I	Color	?	SKP1019BEC	001083909AA8
Centronics Printer/Plotter	RGN I	Color	?	SKP1019CT	1083939073
Centronics Printer/Plotter	RGN I	Color	?	SKP1012EC	0060B02E1E5D
Centronics Printer/Plotter	RGN I	Color	?	SKP1084B	001083F2A7F4
Centronics Printer/Plotter	RGN I	Color	?	SKP1084A	0030C10A5C11
Centronics Printer/Plotter	RGN I	Color	?	SKP1012E	0060B02E1E5D
Centronics Printer/Plotter	RGN I	Color	?	SKP2101-4P	0060B09BCEBC
HP Color LaserJet 5	RGN I	Color	?	SKP1047C	0060B0C92E6B
HP Color LaserJet 5	RGN I	Color	?	SKP1029C	0060B0D4CBF0
HP LaserJet 4000	RGN I	B/W	?	SKPBVH4000	0030C10EA4E9
HP LaserJet 4050	RGN I	B/W	?	SKPMILH4050	001083A33370
HP LaserJet 4V	RGN I	B/W	?	SKP1047V	0060B09A2540
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2089H2	0060B09A2568
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1012H	080009E65C7E
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1014H	080009E1C9ED
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2047H2	080009E69203
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1055H2	080009E526B0
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1049H	080009E684EE
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1003H	080009E74E38
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2005H2	080009D7548C
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2005H1	080009E5ED1A
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2047H1	080009E52689
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2019H	080009E582B5
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2086H2	080009D77441
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2089H1	0060B0ADB9FF
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1055H1	080009E5FC99
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP2086H1	080009E199A9
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1029H1	0060B09A252E
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1029H2	080009E60CE9
HP LaserJet 5Si	RGN I	B/W	24 MB	SKP1113H	0060B09A7A7E

NRC NETWORK PRINTERS

Network Printer	LOCATION	BW/Color	Memory	IPX Name	Hardware Address
HP LaserJet 8100	RGN I	B/W	?	SKP1018-8H	001083926ACF
Unknown Device	RGN I	?	?	SKP1019B-P3	001083909AA8
Unknown Device	RGN I	?	?	SKP1019B-P2	001083909AA8
Unknown Device	RGN I	?	?	SKP1012E2	0060B02E1E5D
Centronics Printer/Plotter	RGN II	Color	?	HP1120C-R2-24T49	0060B0C89112
Centronics Printer/Plotter	RGN II	Color	?	SPECTRA-R2-23T113E	0060B020CFC1
HP DeskJet 1120C	RGN II	Color	?	1120C-R2-24T4	0060B0C881F0
HP DeskJet 1120C	RGN II	Color	?	1120C-R2-23T113	0060B0C8910A
HP LaserJet 4/4M	RGN II	B/W	?	HP4-R2-24T83	080009FBD3B5
HP LaserJet 4 Plus	RGN II	B/W	?	HP4-R2-23T101	080009DFC3D4
HP LaserJet 4 Plus	RGN II	B/W	?	HP4-R2-24T78	0060B0962D57
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T146	080009E5EBCE
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T40	080009E51C4F
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T59	0060B0962D3D
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-23T87	080009E5B86F
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-23T115	080009D82DA0
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T69	0060B09C426E
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-23T60	080009E55C52
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-23T6	080009D8024B
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T104	080009D83D6D
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T32	080009E185C8
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T119	0060B04C5BF4
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-23T67	080009E185C7
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T4	080009E55C58
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-23T72	080009D81D8A
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T135	080009D8023D
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-23T136	080009E5C82E
HP LaserJet 5Si	RGN II	B/W	24 MB	HP5SI-R2-24T84	080009D83D10
HP Color LaserJet 5	RGN III	Color	?	HPLJ5C-R3-3003	080009E536EA
HP Color LaserJet 5M	RGN III	Color	?	HPLJ5C-CH2-4051	080009D734F3
HP Color LaserJet 5M	RGN III	Color	?	HPLJ5C-CH2-4079	080009E66CE5
HP LaserJet 4050	RGN III	B/W	?	SKPOCH4050	0030C10E84F5
HP LaserJet 4Si/4Si MX	RGN III	B/W	18 MB	HPIIISI-CH2-4019	080009D744B9
HP LaserJet 5Si	RGN III	B/W	24 MB	R3-HP8000-2003	0060B061766C
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH1-3082	0060B0E8B5CF
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH1-EICS	080009D76494
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH1-4079A	0060B0AD6EB7
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH2-4045	080009E61CE5
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH1-3112	080009D7346D
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH1-2026	0060B0380659
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SIB-CH2-4079	080009D74489
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH2-4075	080009D74480
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH1-3003	0060B0B993E3
HP LaserJet 5Si	RGN III	B/W	24 MB	SKPIRCH	080009E684E0
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-CH1-3033	0060B05FD11B
HP LaserJet 5Si	RGN III	B/W	24 MB	HP5SI-R350EAST	080009BF45E9
HP LaserJet 8000	RGN III	B/W	?	HP8000_R3_4007	0030C157F6CD
HP LaserJet 8000	RGN III	B/W	?	R3-HP8000-4001	00108372FE5C
HP LaserJet IIISi	RGN III	B/W	?	HPIIISI-CH2-4011	0060B0AD3E01
Centronics Printer/Plotter	RGN IV	Color	?	EP870-R4-PS-425	0060B0C9BE2D
HP Color LaserJet 4500	RGN IV	Color	?	HP_COLOR4500_PS	0010830C9AA7
HP Color LaserJet 5	RGN IV	Color	?	HP5C-R4-PS-457	080009FD5227
HP Color LaserJet 5	RGN IV	Color	?	HP5C-R4-PS-502	080009FD5225
HP Color LaserJet 8500	RGN IV	Color	?	HPC8500-R4-PS-306	001083747DBC
HP Color LaserJet 8500	RGN IV	Color	?	HPC8500-R4-PS-543	00108341AB56
HP Color LaserJet 8500	RGN IV	Color	?	HPC8500-R4-PS-415	0010832BEFB0
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-345	080009E1530A
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-443	080009E5FDFF

NRC NETWORK PRINTERS

Network Printer	LOCATION	BW/Color	Memory	IPX Name	Hardware Address
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP2100M-R4-PS-401	080009E5DD69
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-502	080009E5FCAF
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-527	080009E66C57
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-413	0060B0C9BE2D
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-428	080009D764F3
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-368	080009D734F7
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-304	080009D7546F
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-412	080009F78ED9
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-543	080009E58287
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-452	080009E58338
HP LaserJet 5Si	RGN IV	B/W	24 MB	HP5SI-R4-PS-562	080009E5FC5F
HP LaserJet 5Si	RGN IV	B/W	25 MB	HP5SI-R4-PS-423	0060B0C9BE2D
Centronics Printer/Plotter	?	Color	?	PHASER220-WN-5E05	0060B044BA6C
HP Color LaserJet 5	?	Color	?	?	080009FD2263
Tektronix Network Printer	?	Color	?	?	080011044FCC
Unknown Device	?	Color	?	PHASER-WN-8E02	0060B09AEDF8
Unknown Device	?	Color	?	PHASER-WN-12H03-S	0060B044BA6C
Unknown Device	?	Color	?	PHASER-WN-12H03-P	0060B044BA6C
HP LaserJet 4 Plus	?	B/W	?	HPLASER_SKS	0800099705BF
HP LaserJet 4 Plus	?	B/W	?	HP4M-CIS1-909B	080009E52685
HP LaserJet 4 Plus	?	B/W	?	HP4M_2ND_205_PS	8.00E+17
HP LaserJet 4 Plus	?	B/W	?	HP4M_GRAPHICS_PS	80009900490
HP LaserJet 4 Plus	?	B/W	?	HP4M_4TH_FLR_PS	0800091D6BCC
HP LaserJet 4Si/4Si MX	?	B/W	18 MB	?	0060B0906D09
HP LaserJet 4Si/4Si MX	?	B/W	18 MB	?	0060B0E8C5A9
HP LaserJet 4Si/4Si MX	?	B/W	18 MB	?	0060B09A257B
HP LaserJet 4Si/4Si MX	?	B/W	18 MB	?	00108307D369
HP LaserJet 4Si/4Si MX	?	B/W	18 MB	?	080009D72476
HP LaserJet 4Si/4Si MX	?	B/W	18 MB	?	80009608776
HP LaserJet 4Si/4Si MX	?	B/W	18 MB	?	0800096050AC
HP LaserJet 4Si/4Si MX	?	B/W	18 MB	?	80009608708
HP LaserJet 5Si	?	B/W	24 MB	HP5SI-CIS1-640	080009D734BD
HP LaserJet 5Si	?	B/W	24 MB	HP5SI-NC1	080009E779EC
HP LaserJet 5Si	?	B/W	24 MB	HP5SI_3RD_FLR_PS	080009EB6D4C
HP LaserJet 5Si	?	B/W	24 MB	HP5SI_ADMIN_PS	080009EAAD43
HP LaserJet 5Si	?	B/W	24 MB	?	080009E73E6C
HP LaserJet 5Si	?	B/W	24 MB	HP5SI-CIS1-909A	080009E73E6F
HP LaserJet 5Si	?	B/W	24 MB	?	0060B0C7E90B
HP LaserJet 5Si	?	B/W	24 MB	?	080009AA21C5
HP LaserJet 5Si	?	B/W	24 MB	?	080009D80DE6
HP LaserJet 5Si	?	B/W	24 MB	HP5SI-SAFETY	080009E73ED0
HP LaserJet 5Si	?	B/W	24 MB	?	080009E526F5
HP LaserJet 5Si	?	B/W	24 MB	?	080009AAF924
HP LaserJet 5Si	?	B/W	24 MB	HP5SI_2ND_HALL_PS	0060B0C671B6
HP LaserJet 5Si	?	B/W	24 MB	?	080009D70C28
HP LaserJet 5Si	?	B/W	24 MB	?	0060B09A25A6
HP LaserJet 5Si	?	B/W	24 MB	?	080009D77487
HP LaserJet 5Si	?	B/W	24 MB	?	080009E65C8D
HP LaserJet 5Si	?	B/W	24 MB	HP5SI-CIS1-900	080009D744D2
HP LaserJet 5Si	?	B/W	24 MB	?	080009D754FE
HP LaserJet 5Si	?	B/W	24 MB	?	0060B0C68117
HP LaserJet 8100	?	B/W	?	?	1.08E+07
Unknown Device	?	?	?	NPI2E0ECE_P3	0060B02E0ECE
Unknown Device	?	?	?	NPI9AFDC2_P3	0060B09AFDC2
Unknown Device	?	?	?	?	0060B0FE305B
Unknown Device	?	?	?	NPI939073_P3	1083939073
Unknown Device	?	?	?	?	0060B0731D56
Unknown Device	?	?	?	?	0060B0731D56

NRC NETWORK PRINTERS

Network Printer	LOCATION	BW/Color	Memory	IPX Name	Hardware Address
Unknown Device	?	?	?	NPI2E0ECE_P2	0060B02E0ECE
Unknown Device	?	?	?	NPI319690_P3	0060B0319690
Unknown Device	?	?	?	NPI319690_P2	0060B0319690
Unknown Device	?	?	?	NPI9AFDC2_P2	0060B09AFDC2
Unknown Device	?	?	?	?	0060B0C0D7D5
Unknown Device	?	?	?	?	0010830A15A5
Unknown Device	?	?	?	NPI2E0EAD_P3	0060B02E0EAD
Unknown Device	?	?	?	?	0010830A15A5
Unknown Device	?	?	?	?	0060B0731D56
Unknown Device	?	?	?	?	0010830A15A5
Unknown Device	?	?	?	NPI9AEDF8_P2	0060B09AEDF8
Unknown Device	?	?	?	NPI939073_P2	1083939073
Unknown Device	?	?	?	NPI9AEDF8_P3	0060B09AEDF8
Unknown Device	?	?	?	NPI2DA80A_P3	0060B02DA80A
Unknown Device	?	?	?	NPI2E0EAD_P2	0060B02E0EAD

NRC NETWORK PRINTERS BY MODEL AND LOCATION

Count of Network Printer	LOCATION						
Network Printer	HQ	?	RGN I	RGN II	RGN III	RGN IV	Grand Total
HP LaserJet 5Si	174	20	18	17	13	14	256
HP LaserJet 4Si/4Si MX	54	8			1		63
Unknown Device		24	3				27
Centronics Printer/Plotter	5	1	7	2		1	16
HP Color LaserJet 4500	13					1	14
HP Color LaserJet 5	1	1	2		1	2	7
HP LaserJet 4 Plus		5		2			7
HP Color LaserJet 5M	3				2		5
HP Color LaserJet 8500						3	3
HP LaserJet 4/4M	2			1			3
HP LaserJet 4050	1		1		1		3
HP LaserJet 8100	1	1	1				3
HP Color LaserJet	2						2
HP DeskJet 1120C				2			2
HP LaserJet 8000					2		2
HP 2500C	1						1
HP DeskJet 1220C	1						1
HP DeskJet 1600C	1						1
HP DeskJet 1600CM	1						1
HP LaserJet 4000			1				1
HP LaserJet 4V			1				1
HP LaserJet IIISi					1		1
Tektronix Network Printer		1					1
Grand Total	260	61	34	24	21	21	421

NRC NETWORK PRINTERS BY TYPE AND LOCATION

Count of Network Printer	LOCATION						
BW/Color	HQ	?	RGN I	RGN II	RGN III	RGN IV	Grand Total
B/W	233	34	22	20	18	14	341
Color	27	6	9	4	3	7	56
?		21	3				24
Grand Total	260	61	34	24	21	21	421

NRC SE' R REPORT

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	LOC.	Cost Detail	OS Ver.	Function	Equipment	Memory	CPU SPEED	Model	Processor	IP Address	Hardware SN	Tag Number
2	hqntad01	HQ	DEVL	NT	ADAMS	SERVER	4gig	4x400	PL7000	0	148.184.250.70	D852BWX10150	074160
3	hqntad02	HQ	DEVL	NT	ADAMS	SERVER	4gig	4x400	PL7000	0	148.184.250.71	D852BWX10034	074164
4	hqntad03	HQ	DEVL	NT	ADAMS	SERVER	4gig	4x400	PL7000	0	148.184.250.72	D852BWX10023	074165
5	hqntad04	HQ	DEVL	NT	ADAMS	SERVER	2.25gig	2x450	PL5500	0	148.184.250.73	D909CLD1000	074166
6	hqntad05	HQ	DEVL	NT	ADAMS	SERVER	512mb	2x500	PL1600R	0	148.184.250.74	D930CNK1A698	074167
7	hqntad06	HQ	DEVL	NT	ADAMS	SERVER	4gig	4x400	PL7000	0	148.184.250.75	D852BWX10393	074176
8	hqntad07	HQ	DEVL	NT	ADAMS	SERVER	512mb	2x450	PL1600R	0	148.184.250.76	D903CFX11032	074162
9	hqntad08	HQ	DEVL	NT	ADAMS	SERVER	2gig	8x700	PL8000	0	148.184.250.77	D033FHH1K004	077275
10	hqntad09	HQ	DEVL	NT	ADAMS	SERVER	0	1x500	PL	0	148.184.22.10	0	0
11	NRCADAMS01	HQ	DEVL	NT	ADAMS	SERVER	261mb	2x200	PE6100	0	148.184.157.11	BZ9PJ	065949
12	NRCADAMS03	HQ	DEVL	NT	ADAMS	SERVER	261mb	2x200	PE6100	0	148.184.157.13	BZ9NP	065944
13	NRCADAMS04	HQ	DEVL	NT	ADAMS	SERVER	500mb	4x200	PE6100	0	148.184.157.14	BYV70	065950
14	NRCADAMS05	HQ	DEVL	NT	ADAMS	SERVER	261mb	2x200	PE6100	0	148.184.157.15	BZ9NB	065948
15	NRCADAMS07	HQ	DEVL	NT	ADAMS	SERVER	261mb	2x200	PE6100	0	148.184.157.17	BZ9NH	065947
16	NRCADAMS08	HQ	DEVL	NT	ADAMS	SERVER	261mb	2x200	PE6100	0	148.184.157.18	BZ9NW	065946
17	NRCADAMS09	HQ	DEVL	NT	ADAMS	SERVER	64mb	2x266	PE6100	0	148.184.157.19	BY5MQ	065952
18	NRCADAMS10	HQ	DEVL	NT	ADAMS	SERVER	261mb	2x266	PE2200	0	148.184.157.20	BY5MF	065953
19	NRCADAMS11	HQ	DEVL	NT	ADAMS	SERVER	32mb	200	P200	0	148.184.157.21	CS101479	065216
20	NRCADAMS12	HQ	DEVL	NT	ADAMS	SERVER	32mb	200	P200	0	148.184.157.22	CS101522	065226
21	NRCADAMS13	HQ	DEVL	NT	ADAMS	SERVER	64mb	200	P54C	0	148.184.157.20	104190	067144
22	NRCADAMS14	HQ	DEVL	NT	ADAMS	SERVER	64mb	200	P54C	0	148.184.157.21	104037	067143
23	pbntad01	HQ	DEVL	NT	ADAMS	SERVER							
24	pbntad02	HQ	DEVL	NT	ADAMS	SERVER							
25	pbntad03	HQ	DEVL	NT	ADAMS	SERVER							
26	pbntad04	HQ	DEVL	NT	ADAMS	SERVER							
27	nmss37	HQ	?	AIX 4.2.1	Application	SERVER			IBM H70				
28	nrc_tapps	HQ	Cons	Netware	Application	SERVER							
29	NRC_TAPPS1	HQ	APP GP2	Netware	Application	SERVER	523903 KB	398 MHz	4300	Pentium Pro		U07VB	69780
30	OWFN-3	HQ	Cons	Netware	Application	SERVER	261759 KB	0	4300	Pentium Pro		U07TU	69783
31	ownwas1	HQ	Cons	Netware	Application	SERVER	523903 KB	200 MHz	PowerEdge 6100	Pentium Pro		DCMFQ	67544
32	ownwas2	HQ	APP GP2	Netware	Application	SERVER	523903 KB	332 MHz	ell PowerEdge 42	Pentium Pro		F5VT2	68681
33	SGNWAS1	HQ	Cons	Netware	Application	SERVER	0	0	0	0		0	0
34	twnwas1	HQ	Cons	Netware	Application	SERVER	261759 KB	200 MHz	4300	Pentium Pro		DCMES	67545
35	TWNWAS3	HQ	Cons	Netware	Application	SERVER	523903 KB	400 MHz	ell PowerEdge 63	Pentium Pro		0	0
36	TWNWAS4	HQ	APP GP2	Netware	Application	SERVER	261759 KB	399 MHz	ell PowerEdge 63	Pentium Pro		HGJR0	69518
37	WISP	HQ	Not Priced	Netware	Application	SERVER	15999 KB	66 MHz	Tri-Cor	486 DX		0	47099
38	HQNTAS03	HQ	Cons	NT	Application	SERVER	130mb	200	Computer	0	148.184.14.11	694109-0001	063652
39	HQNTAS06	HQ	Cons	NT	Application	SERVER	261mb	266	PE4200	0	148.184.12.7	FRHRT	068870
40	HQNTAS07	HQ	Cons	NT	Application	SERVER	1gig	2x600	PE2400	0	148.184.14.9	EXRPE	074883
41	HQNTAS2	HQ	Cons	NT	Application	SERVER	130mb	266	NetServer E45	0	148.184.14.10	US82400055	068514
42	hqntas4	HQ	Cons	NT	Application	SERVER	523mb	2x300	PE4200	0	148.184.250.81	E8NZB	067919
43	HQNTAS5	HQ	APP GP2	NT	Application	SERVER	512mb	2x350	PE4200	0	148.184.14.198	GVKRV	069196
44	irm55	HQ	Not Priced	UNIX	Application	SERVER	256M	0	0	0		0	0
45	irm57	HQ	Not Priced	UNIX	Application	SERVER	256M	0	0	0		0	0
46	COMM_ERP	HQ	Not Priced	NT	Auth/Commishoner	SERVER							
47	nrc_root	HQ	Not Priced	Netware	Authentication	SERVER	523903 KB	399 MHz	4300	Pentium Pro		HGJR1	69519
48	EIE	HQ	Not Priced	NT	Authentication	SERVER							
49	EIE2	HQ	Not Priced	NT	Authentication	SERVER							
50	NTBKUP1	HQ	Not Priced	NT	Backup	SERVER							
51	irm70a	HQ	Not Priced	UNIX	Backup	SERVER							
52	hqnwcd1	HQ	File GP2 CD TWR	Netware	CD Tower	SERVER	1048191 KB	398 MHz	0	Pentium Pro		0	0
53	CD1	RGN III	Not Priced	NT	CD Tower	SERVER							
54	R2NTCD01	RGN II	File GP2 CD TWR	NT	CD Tower	SERVER							
55	CTX1A	RGN I	Not Priced	NT	Citrix	SERVER	0	4x200	PE6100	0	148.184.107.12	0	0
56	CTX2A	RGN II	Not Priced	NT	Citrix	SERVER	0	4x200	PE6100	0	148.184.110.12	H98K8	069524

NRC SE' 'R REPORT

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	LOC.	Cost Detail	OS Ver.	Function	Equipment	Memory	CPU SPEED	Model	Processor	IP Address	Hardware SN	Tag Number
57	CTX3A	RGN III	Not Priced	NT	Citrix	SERVER	0	4x200	PE6100	0	148.184.114.12	B79P4	065945
58	CTX4A	RGN IV	Not Priced	NT	Citrix	SERVER	0	4x200	PE6100	0	148.184.105.12	0	0
59	CTXHQA	HQ	Not Priced	NT	Citrix	SERVER	3gig	4x200	PE6100	0	148.184.250.80	B29PX	065943
60	CTXOCM	HQ	Not Priced	NT	Citrix	SERVER	523mb	2x200	PE6100	0	148.184.8.250	C79WS	066417
61	CTXRISE	Rockwall	Not Priced	NT	Citrix (TEST)	SERVER							
62	COMM_ERPCD	HQ	Not Priced	NT	Comm/Authentication	SERVER	96mb	200	Computer	0	148.184.247.25	P200448	068389
63	ERPCD	HQ	Not Priced	NT	Comm/Authentication	SERVER	96mb	200	P54C	0	148.184.247.15	103569	066882
64	HQERPCD1	HQ	Not Priced	NT	Comm/Authentication	SERVER	96mb	200	Computer	0	148.184.247.125	P200446	068387
65	R1_ERPCD	RGN I	Not Priced	NT	Comm/Authentication	SERVER	0	200	P200	0	148.184.107.47	P200538	068309
66	R2_ERPCD	RGN II	Not Priced	NT	Comm/Authentication	SERVER	0	200	0	0	148.184.109.12	0	0
67	R3_ERPCD	RGN III	Not Priced	NT	Comm/Authentication	SERVER	0	200	P200	0	148.184.112.12	P200598	068272
68	R4_ERPCD	RGN IV	Not Priced	NT	Comm/Authentication	SERVER	0	200	0	0	148.184.103.12	0	0
69	DNS1	HQ	App ES2 DMZ	SOLARIS 2.6	DMZ	SERVER			SPARC 5			DNS	
70	DNS2	HQ	App ES2 DMZ	SOLARIS 2.6	DMZ	SERVER			SPARC 5			DNS	
71	DNS3	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SPARC 2			DNS	
72	IDS1	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN UE2			EXTERNAL IDS	
73	IDS2	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN ULTRA 2			DMZ IDS	
74	IGATE	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN SPARC 20			EXTERNAL DNS SMTP GATEWAY TELNET PROXY FTP PROXY, 2nd Socks	
75	IGATE2	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN UE2			PRIMARY SOCKS 2ND SMTP 2ND EX DNS	
76	IGATE3	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SPARC 5			DORMANT NEWS SERVER	
77	IGATE4	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN UE1			PRIMARY DNS FOR WWW.PROXY	
78	IHOST	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SPARC 2			SECURITY	
79	VPN1	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN U2			AVENTAIL VPN	
80	IRM14	HQ	Cons	UNIX	DMZ	SERVER			SUN UE2			SECURITY	
81	IRM70	HQ	Cons	UNIX	DMZ	SERVER			SUN UE2			WEB PROXY	
82	CNNTMD01	TTC	Not Priced	NT	Domain Ctrls	SERVER	512mb	2x333	PE4200	0	148.184.142.15	ETLLH	068473
83	HQNTMD01	HQ	Not Priced	NT	Domain Ctrls	SERVER	654mb	2x333	PE4200	0	148.184.8.6	ETLLB	068479
84	HQNTMD03	HQ	Not Priced	NT	Domain Ctrls	SERVER	654mb	2x333	PE4200	0	148.184.250.92	ETLLC	068478
85	HQNTMD1	HQ	Not Priced	NT	Domain Ctrls	SERVER	64mb	200	P54C	0	148.184.204.12	104169	067147
86	HQNTMD2	HQ	Not Priced	NT	Domain Ctrls	SERVER	64mb	200	P54C	0	148.184.204.13	104162	067145
87	R1NTMD01	RGN I	Not Priced	NT	Domain Ctrls	SERVER	0	2x333	PE4200	0	148.184.107.11	ETLLD	068474
88	R2NTMD01	RGN II	Not Priced	NT	Domain Ctrls	SERVER	0	2x333	PE4200	0	148.184.110.21	ETLLT	068475
89	R3NTMD01	RGN III	Not Priced	NT	Domain Ctrls	SERVER	0	2x333	PE4200	0	148.184.113.12	ETLLG	068476
90	R4NTMD01	RGN IV	Not Priced	NT	Domain Ctrls	SERVER	0	2x333	PE4200	0	148.184.104.11	ETLLR	068477
91	GUIN-NAV	HQ	Not Priced	NT	E-mail virus checker	SERVER	96mb	200	P54C	0	148.184.11.89	104067	067157
92	EBNWFS1	HQ	File GPES2	Netware	File	SERVER	130687 KB	166 MHz	0	Intel Pentium		0	0
93	GDNWFS1	HQ	File GPES2	Netware	File	SERVER	261759 KB	398 MHz	4300	Pentium Pro		U07VP	69789
94	LSNWFS1	HQ	File GPES2	Netware	File	SERVER	130687 KB	166 MHz	0	Intel Pentium		0	0
95	ownwfs1	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	PowerEdge 6100	Pentium Pro		99KZ7	64568
96	ownwfs2	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	PowerEdge 6100	Pentium Pro		99LOZ	64569
97	ownwfs3	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	PowerEdge 6100	Pentium Pro		8V5PS	64025
98	ownwfs4	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	PowerEdge 6100	Pentium Pro		99KWS	64567
99	ownwfs5	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	PowerEdge 6100	Pentium Pro		EVSM7	68482
100	r1nwfs2	RGN I	Reg File GP2	Netware	File	SERVER	261,756 KB	601 MHz	0	0		0	0
101	R2NWFS2	RGN II	Reg File GP2	Netware	File	SERVER	523,903 KB	199 MHz	0	0		0	0
102	r4nwfs2	RGN IV	Reg File GP2	Netware	File	SERVER	589,439 KB	198 MHz	0	0		0	0
103	RWNWFS1	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	PowerEdge 6100	Pentium Pro		CGYVY	66833
104	SGNWFS1	HQ	File GPES2	Netware	File	SERVER	261,756 KB	398 MHz	0	0		0	0
105	SGNWFS1B	HQ	File GPES2	Netware	File	SERVER	0	0	0	0		0	0

NRC SF ER REPORT

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	LOC.	Cost Detail	OS Ver.	Function	Equipment	Memory	CPU SPEED	Model	Processor	IP Address	Hardware SN	Tag Number
106	TTnwfs1	TTC	Reg File GP2	Netware	File	SERVER	523,903 KB	199 MHz	0	0		0	0
107	twnwfs1	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	PowerEdge 6100/	Pentium Pro		99L04	64570
108	twnwfs2	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	4300	Pentium Pro		99KVY	64563
109	twnwfs3	HQ	File GPES2	Netware	File	SERVER	523903 KB	398 MHz	ell PowerEdge 43(	Pentium Pro		U07V6	69784
110	twnwfs4	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	PowerEdge 6100/	Pentium Pro		GT3LL	69236
111	twnwfs5	HQ	File GPES2	Netware	File	SERVER	523903 KB	200 MHz	0	Pentium Pro		99KV3	64564
112	R4NTFS1	RGN IV	Reg File GP2	NT	File	SERVER							
113	R4NTFS4	RGN IV	Cons	NT	File	SERVER							
114	nmss2	HQ	File GPES2	SOLARIS 2.6	File	SERVER	256 MB	0	Sparc 1000	0		351K0249	46724
115	HQNTHD01	HQ	Not Priced	NT	Help Desk	SERVER	523mb	400	PE4300	0	148.184.7.102	U07TX	069778
116	HQNTHD02	HQ	Not Priced	NT	Help Desk	SERVER	523mb	500	Computer	0	148.184.7.104	32103290	076030
117	HQNTHD03	HQ	Not Priced	NT	Help Desk	SERVER							
118	HQNTHD04	HQ	Not Priced	NT	Help Desk	SERVER	523mb	500	Computer	0	148.184.6.15	32103289	076035
119	HQNTHD05	HQ	Not Priced	NT	Help Desk	SERVER							
120	HQNWMS1	HQ	Cons	Netware	Mail	SERVER	130687 KB	166 MHz	Dell PowerEdge XI	Intel Pentium		7BNP6	62537
121	hqnwms2	HQ	Cons	Netware	Mail	SERVER	261759 KB	398 MHz	0	Pentium Pro		0	0
122	ownwms1	HQ	Mail GP2	Netware	Mail	SERVER	523888 KB	864 MHz	ell PowerEdge 44(	Pentium Pro		16K530B	75978
123	ownwms2	HQ	Mail GP2	Netware	Mail	SERVER	523888 KB	864 MHz	ell PowerEdge 44(	Pentium Pro		F5K530B	75979
124	ownwms4	HQ	Mail GP2	Netware	Mail	SERVER	523888 KB	864 MHz	ell PowerEdge 44(	Pentium Pro		C6K530B	75976
125	ownwms5	HQ	Mail GP2	Netware	Mail	SERVER	523888 KB	864 MHz	ell PowerEdge 44(	Pentium Pro		C5K530B	75977
126	R1NWMS1	RGN I	Reg App/Mail GP2	Netware	Mail	SERVER	523,888 KB	864 MHz	0	0		0	0
127	r2nwms1	RGN II	Reg App/Mail GP2	Netware	Mail	SERVER	523,888 KB	864 MHz	0	0		0	0
128	R3NWMS1	RGN III	Reg App/Mail GP2	Netware	Mail	SERVER	261,744 KB	864 MHz	0	0		0	0
129	R4NWMS1	RGN IV	Reg App/Mail GP2	Netware	Mail	SERVER	523,888 KB	864 MHz	0	0		0	0
130	TTnwms2	TTC	Reg App/Mail GP2	Netware	Mail	SERVER							
131	twnwms1	HQ	Cons	Netware	Mail	SERVER	523888 KB	864 MHz	0	Pentium Pro		0	0
132	twnwms2	HQ	Cons	Netware	Mail	SERVER	523888 KB	864 MHz	0	Pentium Pro		0	0
133	twnwms3	HQ	Cons	Netware	Mail	SERVER	523888 KB	864 MHz	0	Pentium Pro		0	0
134	twnwms4	HQ	Cons	Netware	Mail	SERVER	523888 KB	864 MHz	0	Pentium Pro		0	0
135	twnwms5	HQ	Cons	Netware	Mail	SERVER	523888 KB	864 MHz	0	Pentium Pro		0	0
136	DG1	Data Center	Not Priced		Mini-Mainframe	SERVER							
137	DG2	Data Center	Not Priced		Mini-Mainframe	SERVER							
138	OPTIVITY90	HQ	Not Priced	NT	Network Monitoring	SERVER							
139	PROVISION	HQ	Not Priced	NT	Network Monitoring	SERVER							
140	WHATSUPGOLD	HQ	Not Priced	NT	Network Monitoring	SERVER							
141	hpov	HQ	Not Priced	UNIX	Network Monitoring	SERVER							
142	hpov2	HQ	Not Priced	UNIX	Network Monitoring	SERVER							
143	IR400_4TH	HQ	Not Priced	UNIX / NT	Network Monitoring	SERVER							
144	11.23	HQ	Not Priced	NT	Network Support	SERVER							
145	HQNTNS01	HQ	Not Priced	NT	Network Support	SERVER	261mb	400	PE4300	0	148.184.250.36	U07VS	069788
146	HQNTNS02	HQ	Not Priced	NT	Network Support	SERVER	785mb	400	PE4300	0	148.184.250.85	U07V1	069791
147	HQNTNS03	HQ	Not Priced	NT	Network Support	SERVER	654mb	2x333	PE4300	0	148.184.250.23	U07TR	069790
148	VIRTEST	HQ	Not Priced	NT	Network Support	SERVER							
149	CAN600-R4-430	RGN IV	Not Priced	NT	Print	SERVER							
150	HP1	Data Center	Not Priced		Print	SERVER							
151	hp2	Data Center	Not Priced		Print	SERVER							
152	hp3	Data Center	Not Priced		Print	SERVER							
153	irm31	RGN I	?	AIX 4.2.1	Replication	SERVER	256M	0	0	0		0	0
154	irm32	RGN II	?	AIX 4.2.1	Replication	SERVER	256M	0	0	0		0	0
155	irm33	RGN III	?	AIX 4.2.1	Replication	SERVER	256M	0	0	0		0	0
156	irm34	RGN IV	?	AIX 4.2.1	Replication	SERVER	256M	0	0	0		0	0
157	nrr30	HQ	Not Priced	AIX 4.2.1	SQL	SERVER	256M		570				
158	irm30	HQ	Not Priced	UNIX	SQL	SERVER	256M		570				
159	irm35	HQ	?	UNIX	SQL	SERVER	256M		370				
160	irm36	HQ	Not Priced	UNIX	SQL	SERVER	512M		595				

NRC SE[illegible]R REPORT

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	LOC.	Cost Detail	OS Ver.	Function	Equipment	Memory	CPU SPEED	Model	Processor	IP Address	Hardware SN	Tag Number
161	irm37	HQ	?	UNIX	SQL	SERVER	256M		370				
162	irm38	HQ	?	UNIX	SQL	SERVER	256M		360				
163	irm50	HQ	Not Priced	UNIX	SQL	SERVER	256M		580				
164	irm51	HQ	Not Priced	UNIX	SQL	SERVER	256M		580				
165	irm52	HQ	Not Priced	UNIX	SQL	SERVER	256M		390				
166	irm53	HQ	Not Priced	UNIX	SQL	SERVER	256M		591				
167	irm56	HQ	?	UNIX	SQL	SERVER	256M		360				
168	irm59	HQ	?	UNIX	SQL	SERVER	256M		390				
169	irm62	HQ	?	UNIX	SQL	SERVER	256M		370				
170	irm63	HQ	Not Priced	UNIX	SQL	SERVER	512M		595				
171	rps1	RGN I	Not Priced	UNIX	SQL	SERVER	2GB		H70				
172	rps2	RGN II	Not Priced	UNIX	SQL	SERVER	2GB		H70				
173	rps3	RGN III	Not Priced	UNIX	SQL	SERVER	2GB		H70				
174	rps4	RGN IV	Not Priced	UNIX	SQL	SERVER	2GB		H70				
175	rps5	HQ	Not Priced	UNIX	SQL	SERVER	2GB		H70				
176	rps6	HQ	Not Priced	UNIX	SQL	SERVER	2GB		H70				
177	hqnwsf2	HQ	DEVL	Netware	StarFire	SERVER	1048191 KB	200 MHz	PowerEdge 6100	Pentium Pro		G560L	68959
178	hqnwsf4	HQ	DEVL	Netware	StarFire	SERVER							
179	OWNWAS3	HQ	Cons	Netware	StarFire	SERVER	261759 KB	200 MHz	PowerEdge 6100	Pentium Pro		99KW5	64565
180	r1nwfs1	RGN I	Cons	Netware	StarFire	SERVER	523,903 KB	199 MHz	0	0		0	0
181	r2nwfs1	RGN II	Cons	Netware	StarFire	SERVER	523,903 KB	199 MHz	0	0		0	0
182	r3nwfs1	RGN III	Cons	Netware	StarFire	SERVER	523,903 KB	199 MHz	0	0		0	0
183	r4nwfs1	RGN IV	Cons	Netware	StarFire	SERVER	104,191 KB	199 MHz	0	0		0	0
184	ttcnwfs1	TTC	Cons	Netware	StarFire	SERVER							
185	CTXSTARFIRE	HQ	Not Priced	NT	StarFire	SERVER	1gig	4x200	PE6100	0	148.184.43.53	G5958	068958
186	hqntsf1	HQ	DEVL	NT	StarFire	SERVER	523mb	2x333	PE4200	0	148.184.250.63	G3KJH	068960
187	hqntsf2	HQ	DEVL	NT	StarFire	SERVER	1gig	933	PE6100	0	148.184.250.109	G560L	068959
188	cfo1	HQ	Not Priced	UNIX	StarFire	SERVER							
189	cfo1_hme	HQ	Not Priced	UNIX	StarFire	SERVER							
190	cfo2	HQ	Not Priced	UNIX	StarFire	SERVER							
191	cfo3	HQ	Not Priced	UNIX	StarFire	SERVER							
192	HR1	HQ	?	UNIX	StarFire	SERVER	3 Gb	?	SUN E5500				
193	nrr25	HQ	Not Priced	UNIX	StarFire	SERVER							
194	ownwts1	HQ	Not Priced	Netware	Tape Server	SERVER	104191 KB	200 MHz	Dell CPU	Pentium Pro		DCMFK	67548
195	r1nwts1	RGN I	Not Priced	Netware	Tape Server	SERVER	523,903 KB	398 MHz	0	0		0	0
196	r2nwts1	RGN II	Not Priced	Netware	Tape Server	SERVER	261,759 KB	398 MHz	0	0		0	0
197	R3NWTS1	RGN III	Not Priced	Netware	Tape Server	SERVER	261,759 KB	399 MHz	0	0		0	0
198	r4nwts1	RGN IV	Not Priced	Netware	Tape Server	SERVER	0	0	0	0		0	0
199	twnwts1	HQ	Not Priced	Netware	Tape Server	SERVER	1048191 KB	200 MHz	Dell CPU	Pentium Pro		DCMFF	67547
200	NOC1	HQ	Not Priced	Netware	TEST	SERVER	0	0	0	0		0	0
201	NOC2	HQ	Not Priced	Netware	TEST	SERVER	0	0	0	0		0	0
202	NRC_ROOT_TEST	HQ	Not Priced	Netware	TEST	SERVER	0	350 MHz	ell PowerEdge 42	Pentium II		GT3LK	69233
203	NRC_SERVER	HQ	Not Priced	Netware	TEST	SERVER	0	0	0	0		0	0
204	ONWTST1	HQ	Not Priced	Netware	TEST	SERVER	327295 KB	350 MHz	ell PowerEdge 42	Pentium Pro		GT3LM	69234
205	ONWTST2	HQ	Not Priced	Netware	TEST	SERVER	130687 KB	450 MHz	DTK	Pentium Pro		C990034406L	74527
206	R4EXTREME	RGN IV	Not Priced	Netware	TEST	SERVER	0	0	0	0		0	0
207	TNWTST1	HQ	Not Priced	Netware	TEST	SERVER	392831 KB	166 MHz	Dell PowerEdge XI	Intel Pentium		DCMFV	63192
208	TNWTST2	HQ	Not Priced	Netware	TEST	SERVER	261758 KB	166 MHz	Dell PowerEdge XI	Intel Pentium		Z00006812	63194
209	ADAMSTS1	HQ	Not Priced	NT	TEST	SERVER	0	8x700	0	0	148.184.250.68	0	0
210	ADAMSTS2	HQ	Not Priced	NT	TEST	SERVER							
211	Seagate-Info	HQ	Not Priced	NT	TEST	SERVER							
212	hqntop1	HQ	App ES2 Web	NT	WEB	SERVER	1gig	400	PE4300	0	148.184.10.8	HGJVF	069520
213	HQNTWS1	HQ	?	NT	WEB	SERVER	523mb	300	PE4200	0	148.184.204.16	DW3TC	067816
214	R1NTWS1	RGN I	?	NT	WEB	SERVER							
215	R2NTWS1	RGN II	?	NT	WEB	SERVER							

NRC SE' R REPORT

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	**Name**	**LOC.**	**Cost Detail**	**OS Ver.**	**Function**	**Equipment**	**Memory**	**CPU SPEED**	**Model**	**Processor**	**IP Address**	**Hardware SN**	**Tag Number**
216	R3NTWS1	RGN III	?	NT	WEB	SERVER							
217	WWW	HQ	?	SOLARIS 2.6	WEB	SERVER			SUN E3500	PRIMARY EX WEB~2ND SOCKS~2ND EX DNS FOR PR(			
218	IRM12	HQ	App ES2 Web	UNIX	WEB	SERVER			SUN SPARC 1000			INTERNAL WEB	
219	NRCNWC	HQ	?	Netware	?	SERVER	0	0	0	0		0	0
220	rwnwrs1	HQ	?	Netware	?	SERVER	261759 KB	199 MHz	PowerEdge 6100	Pentium Pro		DCMFV	67546
221	INPO	Rockwall	?	NT	?	SERVER	0	200	P54C	0	148.184.43.6	104115	067181
222	R3NTNSA1	RGN III	?	NT	?	SERVER							
223	PAA1	Rockwall	Not Priced	(FIRE-WALL	?	SERVER			CISCO PIX			PAA1 FIREWALL	
224	PAA2	Rockwall	Not Priced	(FIRE-WALL	?	SERVER			CISCO PIX			PAA2 FIREWALL	
225	nmss26	HQ	?	Solaris 2.5.1	?	SERVER	0	0	Sparc 1000e	0		539F14B5	57811
226	nmss999	HQ	?	Solaris 2.5.1	?	SERVER	128 MB	0	Sparc 1000e	0		539F14B6	57807
227	nmss1	HQ	?	SOLARIS 2.6	?	SERVER	512 MB	0	Sparc Ultra 60	0		838F2A1E	69117
228	odin	HQ	?	UNIX	?	SERVER			0			0	0
229	phoenix	HQ	?	UNIX	?	SERVER			0			0	0
230	zeus	HQ	?	UNIX	?	SERVER			0			0	

```
*****************************************************************************
* User name:    glk (55)                        Queue:  TWNWFS2/CN=5SI-T4F38.OU=Q.O=
* File name:                                    Server: HP5SI-T4F38
* Directory:
* Description: 12 Servers.xls
               September 28, 2001                        8:14am
*****************************************************************************
*
*                                      ll   k
*                                       l   k
*                                ggg    l   k  k
*                               g   g   l   k k
*                               g   g   l   kk
*                               g   g   l   k k
*                                gggg  lll  k  k
*                                   g
*                               gggg
*
*****************************************************************************
*
*      55555  SSS   III        TTTTT    4  FFFFF 33333  888          QQQ
*      5     S   S   I           T     44  F        3  8   8        Q   Q
*      5555  S       I           T    4 4  F       3   8   8        Q   Q
*          5  SSS    I   -----   T   4  4  FFFF     3   888         Q   Q
*          5     S   I           T   44444 F         3 8   8        Q Q Q
*      5   5 S   S   I           T      4  F     3   3 8   8  ..    Q  Q
*       555   SSS   III          T      4  F      333   888   ..     QQ Q
*
*
*
*****************************************************************************
```

NRC SERVERS BY TYPE

	A	B	C	D	E	F	G	H	I	J	K	L
1	Equipment	SERVER										
	Count of Name	Cost Detail										
4	Function	Consolidated	DEVL	File GPES2	Reg File GP2	Reg App/Mail GP2	APP GP2	Mail GP2	App ES2 DMZ	App ES2 Web	File GP2 CD TWR	Grand Tot
5	ADAMS		25									
6	File	1		17	5							
7	Application	11					4					
8	StarFire	6	4									
9	Mail	7				5		4				
10	DMZ	11							2			
11	WEB									2		
12	CD Tower										2	
13	Grand Total	36	29	17	5	5	4	4	2	2	2	1(

NRC SERVER CONFIGURATIONS

OS	Item	Manufacturer	Model / Type	Size and Speed
Netware 4.11	System Unit	Dell	Dual processor	
	Motherboard (Bus)			
	CPU	Intel	Pentium Pro III	700 MHz
	RAM			500MB
	Cache			
	Video RAM			
	BIOS			
	Hard Disk			18 GB
	HD Controller Card			
	Floppy Drive			
	Network Interface Card		ATM, optical fiber	
	CD-ROM			
	Video Card			
	Monitor			
	Keyboard			
	Mouse	MS or compatible	PS/2, ver, 2.0A or latest	2 button, 6-pin mini-DIN
	Power Supply		Dual N+1	
	Interfaces Supported		SCSI, PCI	
NT (2-CPU)	System Unit	Dell	Dual processor	
	Motherboard (Bus)			
	CPU	Intel	Pentium Pro III	400 MHz
	RAM			1 GB
	Cache			
	Video RAM			
	BIOS			
	Hard Disk			30 GB
	HD Controller Card			
	Floppy Drive			
	Network Interface Card		ATM, optical fiber	
	CD-ROM			
	Video Card			
	Monitor			
	Keyboard			
	Mouse	MS or compatible	PS/2, ver, 2.0A or latest	2 button, 6-pin mini-DIN
	Power Supply		Dual N+1	
	Interfaces Supported		SCSI, PCI	
	Operating System	MS	NT Server	
NT (4-CPU)	System Unit	Dell	Dual processor	
	Motherboard (Bus)			
	CPU	Intel	Pentium Pro III	400 MHz
	RAM			1 GB
	Cache			
	Video RAM			
	BIOS			
	Hard Disk			30 GB
	HD Controller Card			

NRC SERVER CONFIGURATIONS

	Floppy Drive			
	Network Interface Card		ATM, optical fiber	
	CD-ROM			
	Video Card			
	Monitor			
	Keyboard			
	Mouse	MS or compatible	PS/2, ver, 2.0A or latest	2 button, 6-pin mini-DIN
	Power Supply		Dual N+1	
	Interfaces Supported		SCSI, PCI	
	Operating System	MS	NT Server	
NT (DELL 4-CPU)	System Unit	Dell	Dual processor	
	Motherboard (Bus)			
	CPU	Intel	Pentium Pro III	400 MHz
	RAM			1 GB
	Cache			
	Video RAM			
	BIOS			
	Hard Disk			30 GB
	HD Controller Card			
	Floppy Drive			
	Network Interface Card		ATM, optical fiber	
	CD-ROM			
	Video Card			
	Monitor			
	Keyboard			
	Mouse	MS or compatible	PS/2, ver, 2.0A or latest	2 button, 6-pin mini-DIN
	Power Supply		Dual N+1	
	Interfaces Supported		SCSI, PCI	
	Operating System	MS	NT Server	
Server Type	**Quantities**	**Verified Date**	**Source**	
NetWare Servers	70	7/13/00	M. Williams	
	(70 Dell 2-CPU)			
NT Servers	50	7/13/00	M. Williams	
	(25 Dell 2-CPU)			
	(5 Dell 4-CPU)			
	(15 Compaq 4-CPU)			
	(5 Compaq 8-CPU)			

```
*****************************************************************************
* User name:   glk (55)                      Queue:  TWNWFS2/CN=5SI-T4F38.OU=Q.O=
* File name:                                 Server: HP5SI-T4F38
* Directory:
   escription: 12 Servers.xls
               September 28, 2001                    8:14am
*****************************************************************************
*
*                                     ll   k
*                                      l   k
*                              ggg     l   k  k
*                             g   g    l   k k
*                             g   g    l   kk
*                             g   g    l   k k
*                              gggg   lll  k  k
*                                 g
*                             gggg
*
*****************************************************************************
*
*      55555  SSS   III        TTTTT    4  FFFFF 33333  888          QQQ
*      5     S   S   I           T     44  F        3  8   8        Q   Q
*      5555  S       I           T    4 4  F       3   8   8        Q   Q
*          5  SSS    I   -----   T   4  4  FFFF     3   888         Q   Q
*          5     S   I           T   44444 F         3 8   8        Q Q Q
*      5   5 S   S   I           T      4  F     3   3 8   8  ..    Q  Q
*       555   SSS   III          T      4  F      333   888   ..     QQ Q
*
*
*
    *****************************************************************************
```

NRC NETW COMPONENTS

	A	B	C	E	F	G	H	I	J	M	N
1	Equipment	Name	LOC.	OS Ver.	Function	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
2	HUB	ARBH3A1	RGN IV		ICMP/SNMP						
3	HUB	ARBH3A2	RGN IV		ICMP/SNMP						
4	HUB	ARBH4A1	RGN IV		ICMP/SNMP						
5	HUB	ARBH4A2	RGN IV		ICMP/SNMP						
6	HUB	ARBH5A1	RGN IV		ICMP/SNMP						
7	HUB	ARBH5A2	RGN IV		ICMP/SNMP						
8	HUB	atbh23a1	RGN II		ICMP/SNMP						
9	HUB	atbh23a2	RGN II		ICMP/SNMP						
10	HUB	atbh23b1	RGN II		ICMP/SNMP						
11	HUB	atbh23b2	RGN II		ICMP/SNMP						
12	HUB	atbh24a1	RGN II		ICMP/SNMP						
13	HUB	atbh24a2	RGN II		ICMP/SNMP						
14	HUB	atbh24b1	RGN II		ICMP/SNMP						
15	HUB	atbh24b2	RGN II		ICMP/SNMP						
16	HUB	chbh2a1	RGN III		ICMP/SNMP						
17	HUB	chbh2a2	RGN III		ICMP/SNMP						
18	HUB	chbh3a1	RGN III		ICMP/SNMP						
19	HUB	chbh3a2	RGN III		ICMP/SNMP						
20	HUB	chbh4a1	RGN III		ICMP/SNMP						
21	HUB	chbh4a2	RGN III		ICMP/SNMP						
22	HUB	chbh4b1	RGN III		ICMP/SNMP						
23	HUB	chbh4b2	RGN III		ICMP/SNMP						
24	HUB	cnbh2a1	TTC		ICMP/SNMP						
25	HUB	cnbh2a2	TTC		ICMP/SNMP						
26	HUB	cnbh3a1	TTC		ICMP/SNMP						
27	HUB	cnbh3a2	TTC		ICMP/SNMP						
28	HUB	kpbh1a1	RGN I		ICMP/SNMP						
29	HUB	kpbh1a2	RGN I		ICMP/SNMP						
30	HUB	kpbh1b1	RGN I		ICMP/SNMP						
31	HUB	kpbh1b2	RGN I		ICMP/SNMP						
32	HUB	kpbh2a1	RGN I		ICMP/SNMP						
33	HUB	kpbh2a2	RGN I		ICMP/SNMP						
34	HUB	kpbh2b1	RGN I		ICMP/SNMP						
35	HUB	kpbh2b2	RGN I		ICMP/SNMP						
36	HUB	twbh10a1	HQ		ICMP/SNMP						
37	HUB	twbh10a2	HQ		ICMP/SNMP						
38	HUB	twbh10b1	HQ		ICMP/SNMP						
39	HUB	twbh10b2	HQ		ICMP/SNMP						
40	HUB	twbh2a1	HQ		ICMP/SNMP						
41	HUB	twbh2a2	HQ		ICMP/SNMP						
42	HUB	twbh3a1	HQ		ICMP/SNMP						
43	HUB	twbh3a2	HQ		ICMP/SNMP						
44	HUB	twbh4a1	HQ		ICMP/SNMP						
45	HUB	twbh4a2	HQ		ICMP/SNMP						
46	HUB	twbh4b1	HQ		ICMP/SNMP						
47	HUB	twbh5a1	HQ		ICMP/SNMP						
48	HUB	twbh5a2	HQ		ICMP/SNMP						

NRC NETWC . COMPONENTS

	A	B	C	E	F	G	H	I	J	M	N
1	Equipment	Name	LOC.	OS Ver.	Function	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
49	HUB	twbh6a1	HQ		ICMP/SNMP						
50	HUB	twbh6a2	HQ		ICMP/SNMP						
51	HUB	twbh6b1	HQ		ICMP/SNMP						
52	HUB	twbh6b2	HQ		ICMP/SNMP						
53	HUB	twbh7a1	HQ		ICMP/SNMP						
54	HUB	twbh7a2	HQ		ICMP/SNMP						
55	HUB	twbh7b1	HQ		ICMP/SNMP						
56	HUB	twbh8a2	HQ		ICMP/SNMP						
57	HUB	twbh8b1	HQ		ICMP/SNMP						
58	HUB	twbh8b2	HQ		ICMP/SNMP						
59	HUB	twbh9a2	HQ		ICMP/SNMP						
60	HUB	twbh9b1	HQ		ICMP/SNMP						
61	HUB	twbh9b2	HQ		ICMP/SNMP						
62	HUB	wnbh10a1	HQ		ICMP/SNMP						
63	HUB	wnbh10a2	HQ		ICMP/SNMP						
64	HUB	wnbh11a1	HQ		ICMP/SNMP						
65	HUB	wnbh11a2	HQ		ICMP/SNMP						
66	HUB	wnbh12a1	HQ		ICMP/SNMP						
67	HUB	wnbh12a2	HQ		ICMP/SNMP						
68	HUB	wnbh13a1	HQ		ICMP/SNMP						
69	HUB	wnbh13a2	HQ		ICMP/SNMP						
70	HUB	wnbh14a2	HQ		ICMP/SNMP						
71	HUB	wnbh15a1	HQ		ICMP/SNMP						
72	HUB	wnbh15a2	HQ		ICMP/SNMP						
73	HUB	wnbh16a2	HQ		ICMP/SNMP						
74	HUB	wnbh17a2	HQ		ICMP/SNMP						
75	HUB	wnbh18a1	HQ		ICMP/SNMP						
76	HUB	wnbh2a1	HQ		ICMP/SNMP						
77	HUB	wnbh3a1	HQ		ICMP/SNMP						
78	HUB	wnbh3a2	HQ		ICMP/SNMP						
79	HUB	wnbh4a1	HQ		ICMP/SNMP						
80	HUB	wnbh4a2	HQ		ICMP/SNMP						
81	HUB	wnbh5a2	HQ		ICMP/SNMP						
82	HUB	wnbh6a1	HQ		ICMP/SNMP						
83	HUB	wnbh6a2	HQ		ICMP/SNMP						
84	HUB	wnbh7a1	HQ		ICMP/SNMP						
85	HUB	wnbh7a2	HQ		ICMP/SNMP						
86	HUB	wnbh8a1	HQ		ICMP/SNMP						
87	HUB	wnbh8a2	HQ		ICMP/SNMP						
88	HUB	wnbh9a1	HQ		ICMP/SNMP						
89	HUB	wnbh9a2	HQ		ICMP/SNMP						
90	HUB	wnbhp1a1	HQ		ICMP/SNMP						
91	HUB	wnbhp1a2	HQ		ICMP/SNMP						
92	HUB	LINKSYS Hub	HQ		Unknown			Model EW20HUB		NONE	013284G
93	HUB	twbh5b1	HQ		ICMP/SNMP						
94	HUB	twbh5b2	HQ		ICMP/SNMP						
95	HUB	twbh5c1	HQ		ICMP/SNMP						

NRC NETWO. . COMPONENTS

	A	B	C	E	F	G	H	I	J	M	N
1	Equipment	Name	LOC.	OS Ver.	Function	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
96	HUB	twbh5c2	HQ		ICMP/SNMP						
97	HUB	twbh5d1	HQ		ICMP/SNMP						
98	HUB	twbh5d2	HQ		ICMP/SNMP						
99	HUB	wnbh2b1	HQ		ICMP/SNMP						
100	HUB	wnbh2b2	HQ		ICMP/SNMP						
101	HUB	wnbh2c1	HQ		ICMP/SNMP						
102	HUB	wnbh2c2	HQ		ICMP/SNMP						
103	HUB	wnbh2d1	HQ		ICMP/SNMP						
104	HUB	wnbh2d2	HQ		ICMP/SNMP						
105	Lanbox	2813	HQ		Switch/Router						
106	Lanbox	148.184.93.??	HQ		Switch/Router						
107	Lanbox	ARanh	RGN IV		Switch/Router						
108	Lanbox	BCanh	RGN II		Switch/Router						
109	Lanbox	BFanh	RGN II		Switch/Router						
110	Lanbox	BRanh	RGN II		Switch/Router						
111	Lanbox	BVanh	RGN I		Switch/Router						
112	Lanbox	BWanh	RGN III		Switch/Router						
113	Lanbox	BYanh	RGN III		Switch/Router						
114	Lanbox	CAanh	RGN IV		Switch/Router						
115	Lanbox	CATanh	RGN II		Switch/Router						
116	Lanbox	CCanh	RGN I		Switch/Router						
117	Lanbox	CLanh	RGN III		Switch/Router						
118	Lanbox	COanh	RGN III		Switch/Router						
119	Lanbox	CPanh	RGN IV		Switch/Router						
120	Lanbox	CRanh	RGN II		Switch/Router						
121	Lanbox	CSanh	RGN IV		Switch/Router						
122	Lanbox	DAanh	RGN III		Switch/Router						
123	Lanbox	DBanh	RGN III		Switch/Router						
124	Lanbox	DCanh	RGN IV		Switch/Router						
125	Lanbox	DMZE1	HQ		Switch/Router						
126	Lanbox	DMZE3	HQ		Switch/Router						
127	Lanbox	DMZE4	HQ		Switch/Router						
128	Lanbox	DRanh	RGN III		Switch/Router						
129	Lanbox	ERanh	RGN II		Switch/Router						
130	Lanbox	FAanh	RGN II		Switch/Router						
131	Lanbox	FCanh	RGN IV		Switch/Router						
132	Lanbox	FEanh	RGN III		Switch/Router						
133	Lanbox	FIanh	RGN I		Switch/Router						
134	Lanbox	FNE1	HQ		Switch/Router						
135	Lanbox	FWE1	HQ		Switch/Router						
136	Lanbox	GGanh	RGN IV		Switch/Router						
137	Lanbox	GIanh	RGN I		Switch/Router						
138	Lanbox	HAanh	RGN II		Switch/Router						
139	Lanbox	HATanh	RGN II		Switch/Router						
140	Lanbox	HCanh	RGN I		Switch/Router						
141	Lanbox	IP2anh	RGN I		Switch/Router						
142	Lanbox	IP3anh	RGN I		Switch/Router						

NRC NETWO. . COMPONENTS

	A	B	C	E	F	G	H	I	J	M	N
1	Equipment	Name	LOC.	OS Ver.	Function	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
143	Lanbox	KEanh	RGN III		Switch/Router						
144	Lanbox	Llanh	RGN I		Switch/Router						
145	Lanbox	Liebert 7	HQ		Switch/Router						
146	Lanbox	LSanh	RGN III		Switch/Router						
147	Lanbox	MGanh	RGN II		Switch/Router						
148	Lanbox	MOanh	RGN III		Switch/Router						
149	Lanbox	MSanh	RGN I		Switch/Router						
150	Lanbox	NAanh	RGN II		Switch/Router						
151	Lanbox	NIHE1	HQ		Switch/Router						
152	Lanbox	NManh	RGN I		Switch/Router						
153	Lanbox	OCanh	RGN I		Switch/Router						
154	Lanbox	OCOanh	RGN II		Switch/Router						
155	Lanbox	PAanh	RGN III		Switch/Router						
156	Lanbox	PADanh	RGN III		Switch/Router						
157	Lanbox	PBanh	RGN I		Switch/Router						
158	Lanbox	PBanh	RGN III		Switch/Router						
159	Lanbox	PEanh	RGN III		Switch/Router						
160	Lanbox	Planh	RGN III		Switch/Router						
161	Lanbox	PILanh	RGN I		Switch/Router						
162	Lanbox	POanh	RGN III		Switch/Router						
163	Lanbox	PVanh	RGN IV		Switch/Router						
164	Lanbox	QCanh	RGN III		Switch/Router						
165	Lanbox	RBanh	RGN IV		Switch/Router						
166	Lanbox	ROanh	RGN II		Switch/Router						
167	Lanbox	SBanh	RGN I		Switch/Router						
168	Lanbox	SEanh	RGN II		Switch/Router						
169	Lanbox	SLanh	RGN II		Switch/Router						
170	Lanbox	SOanh	RGN IV		Switch/Router						
171	Lanbox	STanh	RGN IV		Switch/Router						
172	Lanbox	SUanh	RGN I		Switch/Router						
173	Lanbox	SUManh	RGN II		Switch/Router						
174	Lanbox	SURanh	RGN II		Switch/Router						
175	Lanbox	TManh	RGN I		Switch/Router						
176	Lanbox	TPanh	RGN II		Switch/Router						
177	Lanbox	VOanh	RGN II		Switch/Router						
178	Lanbox	VYanh	RGN I		Switch/Router						
179	Lanbox	WBanh	RGN II		Switch/Router						
180	Lanbox	WCanh	RGN IV		Switch/Router						
181	Lanbox	WFanh	RGN IV		Switch/Router						
182	Lanbox	WNPanh	RGN IV		Switch/Router						
183	Mainframe	IBM 3090	HQ		Unknown						
184	NT Peer Server	NTPS	RGN I	NT	Workstation						
185	NT Peer Server	NTPS	RGN I	NT	Workstation						
186	NT Peer Server	NTPS	RGN I	NT	Workstation						
187	NT Peer Server	NTPS	RGN I	NT	Workstation						
188	NT Peer Server	NTPS	RGN I	NT	Workstation						
189	NT Peer Server	NTPS	RGN I	NT	Workstation						

NRC NETWO. . . COMPONENTS

	A	B	C	E	F	G	H	I	J	M	N
1	Equipment	Name	LOC.	OS Ver.	Function	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
190	NT Peer Server	NTPS	RGN I	NT	Workstation						
191	NT Peer Server	NTPS	RGN I	NT	Workstation						
192	NT Peer Server	NTPS	RGN I	NT	Workstation						
193	NT Peer Server	NTPS	RGN I	NT	Workstation						
194	NT Peer Server	NTPS	RGN I	NT	Workstation						
195	NT Peer Server	NTPS	RGN I	NT	Workstation						
196	NT Peer Server	NTPS	RGN I	NT	Workstation						
197	NT Peer Server	NTPS	RGN I	NT	Workstation						
198	NT Peer Server	NTPS	RGN I	NT	Workstation						
199	NT Peer Server	NTPS	RGN I	NT	Workstation						
200	NT Peer Server	NTPS	RGN I	NT	Workstation						
201	NT Peer Server	NTPS	RGN II	NT	Workstation						
202	NT Peer Server	NTPS	RGN II	NT	Workstation						
203	NT Peer Server	NTPS	RGN II	NT	Workstation						
204	NT Peer Server	NTPS	RGN II	NT	Workstation						
205	NT Peer Server	NTPS	RGN II	NT	Workstation						
206	NT Peer Server	NTPS	RGN II	NT	Workstation						
207	NT Peer Server	NTPS	RGN II	NT	Workstation						
208	NT Peer Server	NTPS	RGN II	NT	Workstation						
209	NT Peer Server	NTPS	RGN II	NT	Workstation						
210	NT Peer Server	NTPS	RGN II	NT	Workstation						
211	NT Peer Server	NTPS	RGN II	NT	Workstation						
212	NT Peer Server	NTPS	RGN II	NT	Workstation						
213	NT Peer Server	NTPS	RGN II	NT	Workstation						
214	NT Peer Server	NTPS	RGN II	NT	Workstation						
215	NT Peer Server	NTPS	RGN II	NT	Workstation						
216	NT Peer Server	NTPS	RGN II	NT	Workstation						
217	NT Peer Server	NTPS	RGN II	NT	Workstation						
218	NT Peer Server	NTPS	RGN II	NT	Workstation						
219	NT Peer Server	NTPS	RGN II	NT	Workstation						
220	NT Peer Server	NTPS	RGN II	NT	Workstation						
221	NT Peer Server	NTPS	RGN III	NT	Workstation						
222	NT Peer Server	NTPS	RGN III	NT	Workstation						
223	NT Peer Server	NTPS	RGN III	NT	Workstation						
224	NT Peer Server	NTPS	RGN III	NT	Workstation						
225	NT Peer Server	NTPS	RGN III	NT	Workstation						
226	NT Peer Server	NTPS	RGN III	NT	Workstation						
227	NT Peer Server	NTPS	RGN III	NT	Workstation						
228	NT Peer Server	NTPS	RGN III	NT	Workstation						
229	NT Peer Server	NTPS	RGN III	NT	Workstation						
230	NT Peer Server	NTPS	RGN III	NT	Workstation						
231	NT Peer Server	NTPS	RGN III	NT	Workstation						
232	NT Peer Server	NTPS	RGN III	NT	Workstation						
233	NT Peer Server	NTPS	RGN III	NT	Workstation						
234	NT Peer Server	NTPS	RGN III	NT	Workstation						
235	NT Peer Server	NTPS	RGN III	NT	Workstation						
236	NT Peer Server	NTPS	RGN III	NT	Workstation						

NRC NETWO... COMPONENTS

	A	B	C	E	F	G	H	I	J	M	N
1	Equipment	Name	LOC.	OS Ver.	Function	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
237	NT Peer Server	NTPS	RGN III	NT	Workstation						
238	NT Peer Server	NTPS	RGN III	NT	Workstation						
239	NT Peer Server	NTPS	RGN IV	NT	Workstation						
240	NT Peer Server	NTPS	RGN IV	NT	Workstation						
241	NT Peer Server	NTPS	RGN IV	NT	Workstation						
242	NT Peer Server	NTPS	RGN IV	NT	Workstation						
243	NT Peer Server	NTPS	RGN IV	NT	Workstation						
244	NT Peer Server	NTPS	RGN IV	NT	Workstation						
245	NT Peer Server	NTPS	RGN IV	NT	Workstation						
246	NT Peer Server	NTPS	RGN IV	NT	Workstation						
247	NT Peer Server	NTPS	RGN IV	NT	Workstation						
248	NT Peer Server	NTPS	RGN IV	NT	Workstation						
249	NT Peer Server	NTPS	RGN IV	NT	Workstation						
250	NT Peer Server	NTPS	RGN IV	NT	Workstation						
251	NT Peer Server	NTPS	RGN IV	NT	Workstation						
252	NT Peer Server	NTPS	RGN IV	NT	Workstation						
253	Router	2.1	HQ		Router						
254	Router	4.1	HQ		Router						
255	Router	6.1	HQ		Router						
256	Router	8.1	HQ		Router						
257	Router	10.1	HQ		Router						
258	Router	12.1	HQ		Router						
259	Router	50.1	HQ		Router						
260	Router	50.2	HQ		Router						
261	Router	101.1	HQ		Router						
262	Router	101.3	HQ		Router						
263	Router	136.1	HQ		Router						
264	Router	165.1	HQ		Router						
265	Router	167.1	HQ		Router						
266	Router	169.1	HQ		Router						
267	Router	175.1	HQ		Router						
268	Router	176.1	HQ		Router						
269	Router	180.2	HQ		Router						
270	Router	181.1	HQ		Router						
271	Router	181.2	HQ		Router						
272	Router	182.1	HQ		Router						
273	Router	182.2	HQ		Router						
274	Router	183.1	HQ		Router						
275	Router	183.2	HQ		Router						
276	Router	184.1	HQ		Router						
277	Router	184.2	HQ		Router						
278	Router	185.1	HQ		Router						
279	Router	185.2	HQ		Router						
280	Router	186.1	HQ		Router						
281	Router	186.2	HQ		Router						
282	Router	187.1	HQ		Router						
283	Router	187.2	HQ		Router						

NRC NETWO COMPONENTS

	A	B	C	E	F	G	H	I	J	M	N
1	Equipment	Name	LOC.	OS Ver.	Function	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
284	Router	189.1	HQ		Router						
285	Router	189.2	TTC		Router						
286	Router	190.1	HQ		Router						
287	Router	190.2	TTC		Router						
288	Router	250.1	HQ		Router						
289	Router	csr1	HQ		Router						
290	Router	ebr1	HQ		Router						
291	Router	inr1	HQ		Router						
292	Router	MCI	HQ		Router						
293	Router	NRC5399R1	RGN I		Router						
294	Router	sar1	HQ		Router						
295	Router	tbd	HQ		Router						
296	Router	tbr1	HQ		Router						
297	Router	TWR1	RGN I		Router						
298	Router	TWR1	RGN II		Router						
299	Router	TWR1	RGN III		Router						
300	Router	TWR1	RGN IV		Router						
301	Router	TWR1	TTC		Router						
302	Router	TWR1 93.1	HQ		Router						
303	Router	twr1_16.1	HQ		Router						
304	Router	whr1	HQ		Router						
305	Router	WNR1	RGN I		Router						
306	Router	WNR1	RGN II		Router						
307	Router	WNR1	RGN III		Router						
308	Router	WNR1	RGN IV		Router						
309	Router	WNR1	TTC		Router						
310	Router	WNR4_175.2	HQ		Router						
311	Standalone	MAC	HQ	OS 9.0.4	Standalone	256 MB	0	Power PC-G4	0	0	75985
312	Standalone	SGI	HQ	NT	Standalone			0	0		
313	Workstation	PC_8.20	HQ		StarFire						
314	Workstation	CAC5_16.213	HQ	?	Unknown						
315	?	hera.usnrc.gov	HQ	?	Unknown	?	?	0		0	0
316	?	irix.usnrc.gov	HQ	?	Unknown	?	?	0		0	0
317	?	irm6	HQ	?	Unknown	?	?	0		0	0
318	?	mrxi-2	HQ	?	Unknown	?	?	0		0	0
319	?	ncc1	HQ	?	Unknown	?	?	SUN SPARC 2		0	044981
320	?	noc	HQ	?	Unknown	?	?	SUN SPARC 5		442F3691	052019
321	?	trn1	HQ	?	Unknown	?	?	SUN LX		32902946	044998
322	HOST	cn3	TTC	?	ICMP	0	0	0	0	0	0
323	HOST	irm19	HQ	?	ICMP						
324	HOST	LLNL	HQ	?	ICMP						
325	HOST	UofMD	HQ	?	ICMP						
326	HOST	www.nrc.gov	HQ	?	ICMP						
327	HOST	WWW2	HQ	?	ICMP						
328	HOST	Yahoo	HQ	?	ICMP						

NRC DESKTOP REPORT

MODEL	LOCATION	QTY	RAM	ROCESSOR SEED	Purchase Date	TODAY	AGE (Years)
ADS	HQ	10	128 MB	500 MHZ	9/1/96	7/11/01	4.86
SYLVEST	HQ	695	96 MB	200 MHZ	4/1/97	7/11/01	4.28
SYLVEST	RGN I	70	96 MB	200 MHZ	4/1/97	7/11/01	4.28
SYLVEST	RGN II	62	96 MB	200 MHZ	4/1/97	7/11/01	4.28
SYLVEST	RGN III	103	96 MB	200 MHZ	4/1/97	7/11/01	4.28
SYLVEST	RGN IV	32	96 MB	200 MHZ	4/1/97	7/11/01	4.28
SYLVEST	TTC	15	96 MB	200 MHZ	4/1/97	7/11/01	4.28
GATEWAY	HQ	5	96 MB	200 MHZ	5/1/97	7/11/01	4.20
DYNEX P54C	HQ	1,100	96 MB	200 MHZ	12/1/97	7/11/01	3.61
DYNEX P54C	RGN I	171	96 MB	200 MHZ	12/1/97	7/11/01	3.61
DYNEX P54C	RGN II	99	96 MB	200 MHZ	12/1/97	7/11/01	3.61
DYNEX P54C	RGN III	105	96 MB	200 MHZ	12/1/97	7/11/01	3.61
DYNEX P54C	RGN IV	146	96 MB	200 MHZ	12/1/97	7/11/01	3.61
DYNEX P54C	TTC	30	96 MB	200 MHZ	12/1/97	7/11/01	3.61
QUANTEX	HQ	3	128 MB	266 MHZ	1/1/98	7/11/01	3.53
DYNEX PIO	HQ	73	128 MB	333 MHZ	10/1/98	7/11/01	2.78
DYNEX PIO	RGN I	25	128 MB	333 MHZ	10/1/98	7/11/01	2.78
DYNEX PIO	RGN II	25	128 MB	333 MHZ	10/1/98	7/11/01	2.78
DYNEX PIO	RGN III	25	128 MB	333 MHZ	10/1/98	7/11/01	2.78
DYNEX PIO	RGN IV	25	128 MB	333 MHZ	10/1/98	7/11/01	2.78
DELL	HQ	2	128 MB	600 MHZ	7/1/99	7/11/01	2.03
HP	HQ	2	128 MB	400 MHZ	9/1/99	7/11/01	1.86
DTK	HQ	1,102	128 MB	450 MHZ	10/1/99	7/11/01	1.78
DTK	RGN I	47	128 MB	450 MHZ	10/1/99	7/11/01	1.78
DTK	RGN II	58	128 MB	450 MHZ	10/1/99	7/11/01	1.78
DTK	RGN III	37	128 MB	450 MHZ	10/1/99	7/11/01	1.78
DTK	RGN IV	31	128 MB	450 MHZ	10/1/99	7/11/01	1.78
TRADEMARK	HQ	135	128 MB	350 MHZ	10/1/99	7/11/01	1.78
TRADEMARK	HQ	27	128 MB	350 MHZ	10/1/99	7/11/01	1.78
DYNEX	HQ	60	128 MB	450 MHZ	11/1/99	7/11/01	1.69
DYNEX	TTC	7	128 MB	450 MHZ	11/1/99	7/11/01	1.69
		4,327					

NRC DESKTOPS
SUMMARY BY LOCATION

Sum of QTY	LOCATION						
MODEL	HQ	RGN I	RGN II	RGN III	RGN IV	TTC	Grand Total
DYNEX P54C	1,100	171	99	105	146	30	1,651
DTK	1,102	47	58	37	31		1,275
SYLVEST	695	70	62	103	32	15	977
DYNEX PIO	73	25	25	25	25		173
TRADEMARK	162						162
DYNEX	60					7	67
ADS	10						10
GATEWAY	5						5
QUANTEX	3						3
DELL	2						2
HP	2						2
Grand Total	3,214	313	244	270	234	52	4,327

NRC DESKTOPS
SUMMARY BY OFFICE

OFFICE	LOCATION	FY 2001 FTE	PCs
NRR	HQ	581	663
NMSS	HQ	342	422
RES	HQ	179	256
OCIO	HQ	171	204
OCIO Contractors	HQ	0	286
ADM	HQ	113	185
OCFO	HQ	104	181
HR	HQ	83	204
TTC	TTC	0	65
ACRS/ACNW	HQ	30	63
ASLBP	HQ	21	32
CA	HQ	9	8
CAA	HQ	5	4
COMM	HQ	43	51
EDO	HQ	24	34
IRO	HQ	25	94
OE	HQ	15	18
OGC	HQ	83	95
OI	HQ	42	27
OIG	HQ	44	51
OIP	HQ	25	29
OPA	HQ	14	10
OSP	HQ	19	20
SBCR	HQ	7	10
SECY	HQ	16	21
Region I	RGN I	214	281
Region II	RGN II	197	250
Region III	RGN III	203	325
Region IV	RGN IV	165	300
TOTALS		**2,774**	**4,189**

STANDARD NRC DESKTOP CONFIGURATION

Item	Manufacturer	Model # / Type	Revision or Date	Size and Speed
System Unit		w/ 3 - 5.25" and 2 - 3.5" exposed drive bays		AT Tower
Motherboard	Intel	400BX or 444GX AGP set with PIIX4E South Bridge		100 MHz BUS
CPU	Intel	Pentium III		500 MHz
BIOS		AGP w/ enhanced ACPI, PnP in 2MB Flash EEPROM		
Hard Disk		EIDE UDMA		8.4 GB
HD Controller Card	Integrated on Motherboard			
Floppy Drive				1.44MB 3.5"
Network Interface Card	Bought separately			
CD-ROM		IDE drive		32X
Sound Card	Creative SoundBlaster Link Header			
Speakers	not supplied			
Headset/Microphone	not supplied			
Microphone	not supplied			
Video Card		AGP graphics accelerator card		128-bit
Monitor	View Sonic	Professional Series PS790		19"
Keyboard		w/ PS/2 connector		104 key enhanced
Mouse	MS or compatible	PS/2, ver, 2,0A or latest		2 button, 6-pin mini-DIN
Power Supply		ATX 2.01 compliant		250 watt
Operating System	Microsoft	Windows NT 4.x		

Memory Module Configuration

Item	Manufacturer	MB Total	Type	Speed
RAM		128MB	SDRAM	100MHz
Cache	Intel	512k (L2)		
Video RAM		32MB	AGP, SDRAM	
				Total
				Total w/Monitor

NRC LAPTOP LOANER POOL
(Headquarters)

TAG#	MANUFACTURER	MODEL	PURCHASE DATE
077298	MICRON	SENSPRO850-P111700	10/26/00
072299	MICRON	SENSPRO850-P111700	10/26/00
077300	MICRON	SENSPRO850-P111700	10/26/00
075980	DELL	PPI	7/21/00
074588	DELL	PPX	3/14/00
069044	IBM	2635	9/10/98

UNIX DESKTOPS

Name	LOC.	Cost Detail	OS Ver.	Function	Equipment	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
irm3	HQ		UNIX	?	HP Workstation	64 MB	0	Sparc 10	0	0	45000
nmss3	HQ		Solaris 2.5.1	Client	HP Workstation	64 MB	0	Sparc IPX	0	318M3122	43700
nmss4	HQ		Solaris 2.6	Client	HP Workstation	64 MB	0	Sparc 5	0	535F0BE7	57770
nmss6	HQ		Solaris 2.7	Client	HP Workstation	256 MB	0	Sparc Ultra 10	0	FW93430524	71374
nmss7	HQ		Solaris 2.6	Client	HP Workstation	128 MB	0	Sparc Ultra 1	0	742FCA44	65827
nmss8	HQ		Solaris 2.6	Client	HP Workstation	256 MB	0	Sparc Ultra 10	0	FW84320550	69502
nmss9	HQ		IRIX 6.5	Client	HP Workstation	1024 MB	0	Onyx2	0	K0010312	65822
nmss10	HQ		IRIX 6.5	Client	HP Workstation	256 MB	0	Octane	0	3862A572	69189
nmss11	HQ		Solaris 2.6	Client	HP Workstation	256 MB	0	Sparc Ultra 5	0	FW83930495	69533
nmss12	HQ		Solaris 2.5.1	Client	HP Workstation	64 MB	0	Sparc LX	0	346F2587	46491
nmss13	HQ		Solaris 2.5.1	Client	HP Workstation	32 MB	0	Sparc LX	0	346F2975	46494
nmss14	HQ		Solaris 2.7	Client	HP Workstation	256 MB	0	Sparc Ultra 10	0	FW93430532	71373
nmss15	HQ		Solaris 2.5.1	Client	HP Workstation	32 MB	0	Sparc LX	0	346F3168	46495
nmss16	HQ		Solaris 2.6	Client	HP Workstation	256 MB	0	Sparc Ultra 10	0	FW84320554	69500
nmss17	HQ		Solaris 2.7	Client	HP Workstation	256 MB	0	Sparc Ultra 10	0	FW93430525	71375
nmss18	HQ		Solaris 2.6	Client	HP Workstation	256 MB	0	Sparc Ultra 10	0	FW84320553	69501
nmss19	HQ		Solaris 2.7	Client	HP Workstation	512 MB	0	Sparc Ultra 10	0	FW93740432	71939
nmss20	HQ		Solaris 2.5.1	Client	HP Workstation	64 MB	0	Sparc 5	0	435F4395	51818
nmss21	HQ		Solaris 2.5.1	Client	HP Workstation	64 MB	0	Sparc 5	0	435F4393	51815
nmss22	HQ		Solaris 2.5.1	Client	HP Workstation	256 MB	0	Sparc 20	0	54F0CA3	57870
nmss23	HQ		Solaris 2.6	Client	HP Workstation	128 MB	0	Sparc Ultra 5	0	FW83930722	69192
nmssweb/nmss24	HQ		Solaris 2.6	Client	HP Workstation	256 MB	0	Sparc 20	0	541F07F6	57868
nmss27	HQ		Solaris 2.5.1	Client	HP Workstation	128 MB	0	Sparc Ultra 1	0	628F01D6	61637
nmss28	HQ		Solaris 2.5.1	Client	HP Workstation	256 MB	0	Sparc Ultra 1	0	629F01C0	61612
nmss29	HQ		Solaris 2.6	Client	HP Workstation	256 MB	0	Sparc Ultra 10	0	FW84320594	69499
nmss30	HQ		AIX 4.2.1	Client	HP Workstation	0	0	RS6000	0	0	0
nmss31	HQ		Solaris 2.5.1	Client	HP Workstation	64 MB	0	Sparc 5	0	435F4398	51817
nmss32	HQ		AIX 4.2.1	Client	HP Workstation	512 MB	0	580	0	0	0
nmss33	HQ		AIX 4.2.1	Client	HP Workstation	128 MB	0	580	0	0	0
nmss34	HQ		Solaris 2.6	Client	HP Workstation	?	0	Sparc Ultra 60	0	10212971	60982
nmss35	HQ		Solaris 2.6	Client	HP Workstation	64 MB	0	Sparc 10	0	237F1838	41043
nmss36	HQ		Solaris 2.6	Client	HP Workstation	256 MB	0	Sparc Ultra 60	0	FW02540097	75951
nmsslinux	HQ		Red Hat 6.2	Client	HP Workstation	256 MB	0	0	0	0	75071
nmss5	HQ		Solaris 2.5.1	Client	HP Workstation	64 MB	0	Sparc IPX	0	319M2234	43702
res0	HQ		IRIX 6.5.4m	Client	HP Workstation			SGI Origin 2000 Rack		K0022594	072732
res1	HQ		Solaris 2.5.1	Client	HP Workstation			SUN SPARC 20		436F3622	051833
res2	HQ		Solaris 2.7	Client	HP Workstation			SUN ULTRA 5		FW92410857 (PG)	070984
res3	HQ		Solaris 2.5.1	Client	HP Workstation			SUN SPARC 10		320F1894	043680
res4	HQ		HP-UX 10.20	Client	HP Workstation			HP-C160		US67385266	065772
res5	HQ		Solaris 7	Client	HP Workstation			SUN E5500		932H4427	075943
res6	HQ		Solaris 2.6	Client	HP Workstation			SUN SPARC 10		337F1546	046458
res7	HQ		Solaris 2.6	Client	HP Workstation			SUN SPARC 10		343F0840	046457
res8	HQ		Solaris 7	Client	HP Workstation			SUN ULTRA-5		FW91550240 (PG)	070405

UNIX DESKTOPS

Name	LOC.	Cost Detail	OS Ver.	Function	Equipment	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
res9	HQ		IRIX 6.5.3f	Client	HP Workstation			SGI O2		0800690-5A9BE	068506
res10	HQ		Solaris 2.6	Client	HP Workstation			SUN SPARC 20		439F3712	052330
res11	HQ		Solaris 7	Client	HP Workstation			SUN ULTRA-5		FW92410879 (PG)	070985
res12	HQ		IRIX 6.5.6	Client	HP Workstation			SGI Octane		0800690-BA0B(	065323
res13	HQ		?	Client	HP Workstation		Transfer to N.O.C. - 5/31/2000			-	-
res14	HQ		Solaris 2.5.1	Client	HP Workstation			SUN SPARC 10		321F0370	044667
res15	HQ		Solaris 8	Client	HP Workstation			SUN Ultra 1		623F0D81	059764
res16	HQ		Solaris 2.5.1	Client	HP Workstation			SUN SPARC 10		345F1357	046459
res17	HQ		?	Client	HP Workstation		Transfer to N.O.C. - 5/31/2000			-	-
res18	HQ		Solaris 2.7	Client	HP Workstation			SUN SPARC 5		442F3810	052021
res19	HQ		?	Client	HP Workstation		Transfer to ISL - 2/28/2000			-	-
res20	HQ		Solaris 2.6	Client	HP Workstation			SUN SPARC 20		623F0E5D	059763
res21	HQ		Solaris 2.5.1	Client	HP Workstation			SUN SPARC 20		632F1272	061795
res22	HQ		Solaris 8	Client	HP Workstation			SUN Ultra 1		623F0DA1	059765
res23	HQ		?	Client	HP Workstation		Transfer to ISL - 2/28/2000			-	-
res24	HQ		?	Client	HP Workstation		Transfer to ISL - 2/28/2000			-	-
res25	HQ		Solaris 2.5.1	Client	HP Workstation			SUN Ultra 2		711F1113	063980
res26	HQ		IRIX 6.5.9f	Client	HP Workstation			SGI Octane(SI)		0800690-B7EB9	065011
res27	HQ		Solaris 7	Client	HP Workstation			SUN ULTRA 5		FW92410896 (PG)	070986
res28	HQ		?	Client	HP Workstation		TO SURPLUS - 4/5/2000			-	-
res29	HQ		IRIX 6.5.4f	Client	HP Workstation			SGI Octane		0800690-BA09F	065325
res30	HQ		OSF1 V4.0E	Client	HP Workstation		DEC 8400 A / Compaq GS140			NI72502PXT	065062
res31	HQ		IRIX 6.5.6f	Client	HP Workstation			SGI Octane		0800690-BA06D	065324
res32	HQ		IRIX 6.5.5f	Client	HP Workstation			SGI Octane		0800690-BA069	065329
res33	HQ		IRIX 6.5.6f	Client	HP Workstation			SGI Octane		0800690-BA083	065326
res34	HQ		IRIX 6.5.6f	Client	HP Workstation			SGI Octane		0800690-B74B(	065327
res35	HQ		IRIX 6.5.6f	Client	HP Workstation			SGI Octane		0800690-BA09D	065328
res36	HQ		IRIX 6.5.6f	Client	HP Workstation			SGI Octane		0800690-BA0A/	065322
res37	HQ		HP-UX 10.20	Client	HP Workstation			HP C180-XP		US67385417	065769
res38	HQ		Solaris 7	Client	HP Workstation			SUN ULTRA-5		FW92410806 (PG)	070983
res39	HQ		Solaris 2.6	Client	HP Workstation			SUN Ultra 30		838F2A7C	069134
res40	HQ		IRIX6.5.3f	Client	HP Workstation			SGI Origin 2000 DS		K0014915	068510
res41	HQ		OSF1 V4.0E	Client	HP Workstation			DEC 500 A		NI73902K8V	065756
MAC	HQ		OS 9.0.4	Standalone	Standalone	256 MB	0	Power PC-G4	0	0	75985
mrxi-2	HQ		UNIX	?	?			0		0	0
irix.usnrc.gov	HQ		UNIX	?	?			0		0	0
hera.usnrc.gov	HQ		UNIX	?	?			0		0	0
noc	HQ		UNIX	?	?			SUN SPARC 5		442F3691	052019
ncc1	HQ		UNIX	?	?			SUN SPARC 2		0	044981
irm6	HQ		UNIX	?	?			0		0	0
trn1	HQ		UNIX	?	?			SUN LX		32902946	044998

UNIX RVERS

Name	LOC.	Cost Detail	OS Ver.	Function	Equipment	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
nmss1	HQ	?	Solaris 2.6	?	SERVER	512 MB	0	Sparc Ultra 60	0	838F2A1E	69117
nmss999	HQ	?	Solaris 2.5.1	?	SERVER	128 MB	0	Sparc 1000e	0	539F14B6	57807
nmss26	HQ	?	Solaris 2.5.1	?	SERVER	0	0	Sparc 1000e	0	539F14B5	57811
phoenix	HQ	?	UNIX	?	SERVER			0		0	0
odin	HQ	?	UNIX	?	SERVER			0		0	0
zeus	HQ	?	UNIX	?	SERVER			0		0	#N/A
PAA1	ROCKWALL	Not Priced	PIX FIRE-WALL 5.2	?	SERVER			CISCO PIX		PAA1 FIREWALL	
PAA2	ROCKWALL	Not Priced	PIX FIRE-WALL 5.2	?	SERVER			CISCO PIX		PAA2 FIREWALL	
nmss37	HQ	?	AIX 4.2.1	Application	SERVER			IBM H70			
irm55	HQ	Not Priced	UNIX	Application	SERVER	256M	0	0	0	0	0
rps5e	HQ	Not Priced	UNIX	Application	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
irm57	HQ	Not Priced	UNIX	Application	SERVER	256M	0	0	0	0	0
rps2a	HQ	Not Priced	UNIX	Application	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
rps6e	HQ	Not Priced	UNIX	Application	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
irm70a	HQ	Not Priced	UNIX	Backup	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
DNS1	HQ	pp ES2 DM	SOLARIS 2.6	DMZ	SERVER			SPARC 5		DNS	
DNS2	HQ	pp ES2 DM	SOLARIS 2.6	DMZ	SERVER			SPARC 5		DNS	
DNS3	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SPARC 2		DNS	
IDS1	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN UE2		EXTERNAL IDS	
IDS2	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN ULTRA 2		DMZ IDS	
IRM14	HQ	Cons	UNIX	DMZ	SERVER			SUN UE2		SECURITY	
IRM70	HQ	Cons	UNIX	DMZ	SERVER			SUN UE2		WEB PROXY	
IGATE	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN SPARC 20		EXTERNAL DNS SMTP GATEWAY TELNET PROXY FTP PROXY, 2nd Socks	
IGATE2	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN UE2		PRIMARY SOCKS 2ND SMTP 2ND EX DNS	
IGATE3	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SPARC 5		DORMANT NEWS SERVER	
IGATE4	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN UE1		PRIMARY DNS FOR WWW.PROXY	
IHOST	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SPARC 2		SECURITY	

UNIX RVERS

Name	LOC.	Cost Detail	OS Ver.	Function	Equipment	Memory	CPU SPEED	Model	Processor	Hardware SN	Tag Number
VPN1	HQ	Cons	SOLARIS 2.6	DMZ	SERVER			SUN U2		AVENTAIL VPN	
nmss2	HQ	File GPES2	Solaris 2.6	File	SERVER	256 MB	0	Sparc 1000	0	351K0249	46724
hpov	HQ	Not Priced	UNIX	Network Monitoring	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
hpov2	HQ	Not Priced	UNIX	Network Monitoring	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
irm31	RGN I	?	AIX 4.2.1	Replication	SERVER	256M	0	0	0	0	0
irm32	RGN II	?	AIX 4.2.1	Replication	SERVER	256M	0	0	0	0	0
irm33	RGN III	?	AIX 4.2.1	Replication	SERVER	256M	0	0	0	0	0
irm34	RGN IV	?	AIX 4.2.1	Replication	SERVER	256M	0	0	0	0	0
irm37	HQ	?	UNIX	SQL	SERVER	256M		370			
irm56	HQ	?	UNIX	SQL	SERVER	256M		360			
irm59	HQ	?	UNIX	SQL	SERVER	256M		390			
irm38	HQ	?	UNIX	SQL	SERVER	256M		360			
irm62	HQ	?	UNIX	SQL	SERVER	256M		370			
irm35	HQ	?	UNIX	SQL	SERVER	256M		370			
irm30	HQ	Not Priced	UNIX	SQL	SERVER	256M		570			
irm36	HQ	Not Priced	UNIX	SQL	SERVER	512M		595			
irm63	HQ	Not Priced	UNIX	SQL	SERVER	512M		595			
nrr30	HQ	Not Priced	AIX 4.2.1	SQL	SERVER	256M		570			
rps1	RGN I	Not Priced	UNIX	SQL	SERVER	2GB		H70			
rps2	RGN II	Not Priced	UNIX	SQL	SERVER	2GB		H70			
rps3	RGN III	Not Priced	UNIX	SQL	SERVER	2GB		H70			
rps4	RGN IV	Not Priced	UNIX	SQL	SERVER	2GB		H70			
rps5	HQ	Not Priced	UNIX	SQL	SERVER	2GB		H70			
rps6	HQ	Not Priced	UNIX	SQL	SERVER	2GB		H70			
irm52	HQ	Not Priced	UNIX	SQL	SERVER	256M		390			
irm53	HQ	Not Priced	UNIX	SQL	SERVER	256M		591			
irm50	HQ	Not Priced	UNIX	SQL	SERVER	256M		580			
irm51	HQ	Not Priced	UNIX	SQL	SERVER	256M		580			
HR1	HQ	?	UNIX	StarFire	SERVER	3 Gb	?	SUN E5500			
cfo3	HQ	Not Priced	UNIX	StarFire	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
cfo2	HQ	Not Priced	UNIX	StarFire	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
cfo1	HQ	Not Priced	UNIX	StarFire	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
cfo1_hme	HQ	Not Priced	UNIX	StarFire	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
nrr25	HQ	Not Priced	UNIX	StarFire	SERVER	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
WWW	HQ	?	SOLARIS 2.6	WEB	SERVER			SUN E3500		PRIMARY EX WEB 2ND SOCKS 2ND EX DNS FOR PROXY	
IRM12	HQ	pp ES2 We	UNIX	WEB	SERVER			SUN SPARC 1000		INTERNAL WEB	
MAC	HQ		OS 9.0.4	Standalone	Standalone	256 MB	0	Power PC-G4	0	0	75985

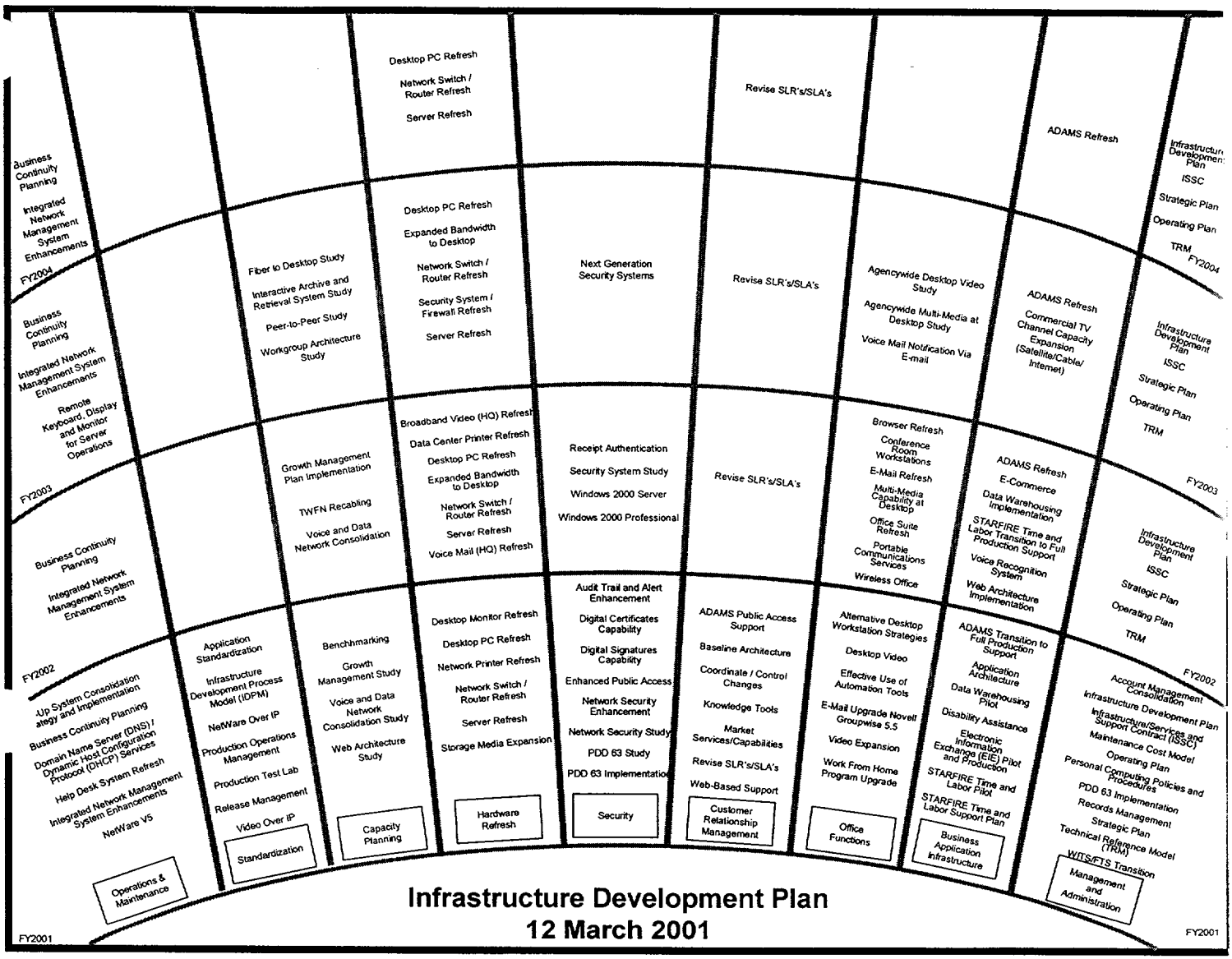
Prepared for:

United States
Nuclear Regulatory Commission
Office of the Chief Information Officer
Information Technology Infrastructure Division

Information Technology Infrastructure Division

Infrastructure Development Forecast Fiscal Years 2001 - 2004

March 12, 2001



Infrastructure Development Plan
12 March 2001

TABLE OF CONTENTS

Introduction 2

1.0 Operations and Maintenance Programs 3

2.0 Standardization Programs 5

3.0 Capacity Planning Programs 7

4.0 Hardware Refresh Programs 9

5.0 Security Programs 12

6.0 Customer Relationship Management Programs 14

7.0 Office Function Programs 16

8.0 Business Application Infrastructure Programs 19

9.0 Management and Administration Programs 22

INFRASTRUCTURE DEVELOPMENT FORECAST-AT-A-GLANCE 24

SUBJECT INDEX 23

Introduction

Division Responsibilities

The Information Technology Infrastructure Division (ITID) provides the planning, design, acquisition, development, integration, implementation, operation, management, and support of the U. S. Nuclear Regulatory Commission's (NRC) information technology (IT) infrastructure. The infrastructure includes the telephones, computers, networks, and computer and telecommunications services required by the agency. It also provides local IT infrastructure support for agency facilities in the Washington Metropolitan Area (WMA).

ITID's responsibilities include the selection, design, implementation, operation, and support of the strategic technologies that comprise the IT infrastructure. Also included in these responsibilities are the establishment of agencywide standard methods and procedures for satisfying common IT requirements.

Purpose of this Document

This document provides an overview of the four year forecast for Infrastructure Development. It contains brief descriptions of the major programs that are under way or forecasted for future years, with an approximation of the year in which each will be planned and implemented. This document is primarily a budget forecasting tool, and is not intended to replace the Operating Plan, which describes the programs that have been approved and scheduled for implementation. Some of the programs forecasted in this document may be replaced by new requirements or technological advances, scheduled earlier, or postponed as the time approaches, business needs change and near term schedules are developed.

Organization

The document contains an introduction, nine categories of programs, a graphic that is shows the forecast-at-a-glance, and a subject index. The nine program categories are:

1.0 Operations and Maintenance
2.0 Standardization
3.0 Capacity Planning
4.0 Hardware Refresh
5.0 Security
6.0 Customer Relationship Management
7.0 Office Functions
8.0 Business Applications Infrastructure
9.0 Management and Administration

Most programs affect more than one category. However, for the sake of simplicity, each program has been placed in the area which it most directly affects. Each section contains a definition of the category or program area and a list and brief description of the projects associated with that area for each of the years 2001 through 2004. Projects are listed in alphabetical order within a given year. At the end of the document is a graphic that depicts the forecast-at-a glance, commonly referred to as the "windshield", and a subject index.

1.0 Operations and Maintenance Programs

1.1 Description

The programs within the Operations and Maintenance program area include those projects which ITID executes to provide continuing operational and maintenance support to the IT infrastructure systems.

1.2 Programs

1.2.1 Fiscal Year 2001

Back-up System Consolidation Strategy and Implementation: This program will develop a strategy and plan to consolidate NRC's two electronic data storage back-up systems into a single system. NRC currently uses two different systems to back up data on its servers. One system is used for backing up network servers, the other is used for backing up the application servers that support the Agency Document Access and Management System (ADAMS). The objective of this program is to reduce the operational support effort needed to perform back-ups and to maintain the back-up systems. In addition, as part of this program, there will be some consideration of the possibility of expanding ITID's back-up services to additional server systems, and possibly desktop systems as appropriate. The implementation of the consolidated back-up system is expected to be completed in Fiscal Year 2001.

Business Continuity Planning: This program will develop a plan for providing continuity of NRC systems operations in the event of a disaster occurring at headquarters. Critical systems will be identified and a plan will be developed to conduct a staged implementation of disaster recovery systems and plans. The plan will include an initial implementation of systems and services necessary to maintain inter-regional communications for office automation, E-Mail, and Internet functions in the event of a loss of the headquarters hub site.

Domain Name Server (DNS) / Dynamic Host Configuration Protocol (DHCP): This program will implement the Novell™ Domain Name Server (DNS) / Dynamic Host Configuration Protocol (DHCP) Services on the agency network. The implementation of DNS/DHCP will decrease the administrative overhead associated with manually assigning network addresses for each of the agency's desktop, application, and server systems. The system will automatically assign addresses and update the appropriate systems. It also consolidates the addressing into a single database instead of the multiple tables and databases that are manually maintained today. DNS / DHCP also allows the re-use of addresses on systems that are idle which effectively increases the total number of systems that may be connected to the agency network.

Help Desk System Refresh: This program will re-design and upgrade the Help Desk trouble reporting system in order to improve the agency's ability to respond to trouble reports on infrastructure systems. One of the primary objectives of this upgrade is to enable the agency to preserve historical data on IT problems for longer periods of time in order to improve its ability to perform status reporting, measurements, and trend analysis. Another objective is to improve the ease of use of the system and increase the automation of common help desk processes. The

Network Associates, Inc. Magic Total Service Desk suite of products will be installed in Fiscal Year 2001 to replace the McAfee Help Desk system that is currently in use.

Integrated Network Management System (INMS) Enhancements: This program will develop requirements, design, procure, integrate, and implement Integrated Network Management System (INMS) enhancements that will ensure that NRC has the ability to monitor, maintain and manage the agency network resources. The system provides availability and status reporting, early warning of problems, and automated recovery. Enhancements will continue to be made in methods to record and measure network performance. In Fiscal Year 2001, What's Up Gold (WUG) will be implemented, the continued use of HewlettPackard's OpenView on Unix will be studied and compared to migration to NT and the use of Optivity software, along with some other potential changes and enhancements to increase the reporting and monitoring capabilities.

NetWare V5: This program will upgrade the network NetWare software on the desktop systems and servers to Version 5. This upgrade will increase the speed and efficiency of the network connections and improve the security capabilities of the systems. NetWare V5 also enhances the ability of the network to communicate with new protocols and new equipment.

1.2.2 Fiscal Year 2002

Business Continuity Planning: (Continued from Fiscal Year 2001).

Integrated Network Management System (INMS) Enhancements; (Continued from Fiscal Year 2001).

1.2.3 Fiscal Year 2003

Business Continuity Planning: (Continued from Fiscal Year 2002).

Integrated Network Management System (INMS) Enhancements; (Continued from Fiscal Year 2002).

Remote Keyboard, Display, and Monitor for Remote Server Operations - Study: Consider the possible use of Keyboard, Display and Mouse (KDM) systems for remote server operational support, particularly at Resident Inspector locations and the regions.

1.2.4 Fiscal Year 2004

Business Continuity Planning: (Continued from Fiscal Year 2003).

Integrated Network Management System (INMS) Enhancements; (Continued from Fiscal Year 2003).

2.0 Standardization Programs

2.1 Description

Programs within the Standardization category represent a continuation of the standardization program at NRC that ensures the compatibility, support ability, and interoperability of the NRC systems and applications. The standardization programs will continue to minimize as much as possible, the number of different hardware and software systems that are performing similar functions in the agency. NRC has designated standard systems and protocols to be used in any new implementations. The standardization programs are intended to minimize the number of different maintenance and support resource skills. Standardization efforts encompass application development issues, network and desktop resources, as well as deployed protocol issues.

2.2 Programs

2.2.1 Fiscal Year 2001

Application Standardization: The goal of this program is to improve efficiency by reducing the need to maintain multiple legacy operating environments. This program will continue the process of modifying and certifying existing in-house applications in order to provide continued support for these applications in the NRC production operations environment. The objective of this program is to implement standardized applications interfaces and ensure that older applications will function in the new desktop environment. Applications that cannot be certified will be retired or replaced in order to provide a stable and uniform applications maintenance and support environment, reduce the potential of software conflicts, and facilitate interoperability.

Infrastructure Development Process Model (IDPM): This program will provide a set of guidelines with the optimum methods for developing new and modifing existing technology, while maintaining the stability and reliability of the infrastructure. Standardized and repeatable processes will be used in the IDPM. This program is continued from Fiscal Year 2000.

NetWare Over IP: With this program, the agency will expand the implementation of IP in order to exclusively use TCP/IP, the dominant Internet protocol, within the NRC networks, reducing the agency's reliance upon older technologies and platforms, such as NetWare IPX.

Production Operations Management: This program will develop a process and design a Production Test Lab environment that will be used to test application software, commercial software, and hardware prior to introducing it into the production operations environment. The process for certifying application software will be implemented in Fiscal Year 2001 with the Production Test Lab. This program is continued from Fiscal Year 2000.

Production Test Lab: This program will formalize the certification and distribution process for implementing agency developed applications as well as the rollout of Commercial Off The Shelf (COTS) software and hardware, through the use of a Production Test Lab. The test lab will be used to certiFiscal Year the production readiness of application software, commercial software, and hardware. It will also be used to pre-test the distribution and installation procedures to be

used for new software and hardware. Regression testing will also be performed in the Lab to ensure that other systems and applications are not affected by the proposed installation.

Release Management: This program will study the hardware and software release and distribution requirements for the agency, and recommend, develop, and implement a Release Management process that will provide controls for ensuring that releases are coordinated, tested, approved, and scheduled for systems, servers and desktop systems. This will be integrated with a process for controlling configurations for all systems. This program is continued from Fiscal Year 2000.

Video / Data Network Consolidation (Video over IP): This program will consolidate the separate video and data networks between NRC headquarters and the regional offices into a single unified network that uses Asynchronous Transmission Mode (ATM) technology and the Internet Protocol (IP). The current Wide Area ATM network, used for data transmission, will be expanded to accommodate video transmissions. After implementation, the NRC will discontinue the separate Wide Area T1 network that is currently used to carry video traffic. This program is continued from Fiscal Year 2000.

2.2.2 Fiscal Year 2002

No programs.

2.2.3 Fiscal Year 2003

No programs.

2.2.4 Fiscal Year 2004

No programs.

3.0 Capacity Planning Programs

3.1 Description

ITID currently supports a variety of systems with a wide variety of applications. This program is intended to implement a regular, on-going program to monitor the use of these systems in order to identiFiscal Year trends and new requirements for system capacity in the areas of permanent and removable storage media, memory size, memory and processor speeds, bus speeds, network bandwidth, number of processors, etc.. Potential procedures and systems will be considered for identifying acceptable thresholds, measuring system usage, alerting support personnel when these thresholds are reached or exceeded, and recording the time, number of occurrences and the duration of the occurrences. This information will be collected and analyzed to provide an early warning system for making recommendations on future required capacity improvements to prevent the degradation of service levels as usage increases.

3.2 Programs

3.2.1 Fiscal Year 2001

Benchmarking: This program will plan, develop, and implement a system to provide benchmarking of new system software and hardware. Benchmarking criteria will be developed for acceptance of new systems into the infrastructure environment. This program is continued from Fiscal Year 2000.

Growth Management Study: This program will perform a Growth Management Study to identiFiscal Year NRC's requirements for growth management and the potential benefits. A Growth Management Plan will be developed that outlines a process for identifying and responding to the NRC's growing demand for IT resources. The implementation of an automated growth management system will be considered. A growth management system would monitor system usage to enable the agency to identiFiscal Year growth trends. By monitoring and reporting the growth in usage of various components of the infrastructure, ITID may better anticipate the agency's requirements for additional capacity before it becomes critical and affects service levels and user productivity. This in turn would allow the agency to plan and budget for system upgrades or replacements. It would also provide more detailed usage information that would allow the agency to identiFiscal Year the components creating bottlenecks to a lower level of granularity in order to plan for staged upgrades instead of complete system replacements. This program will investigate the various growth management systems that are available on the market and determine whether such a system could pay for itself in reduced system acquisition costs, improved productivity, reduced support costs, and improved performance of ITID systems. This program is continued from Fiscal Year 2000.

Voice and Data Network Consolidation Study: This program will study the potential for using new technologies to transport voice and data traffic throughout the agency using a shared media and protocol. The study will recommend for consolidation where appropriate to minimize service charges and support costs. At this time, the voice and data networks are separate systems that use different technologies and protocols. The emergence of newer technologies from the carrier services that provide a common transport protocol at a high bandwidth introduces the potential for gaining some cost savings in this area.

Web Architecture Study: This program will study the possible re-design of the web-based system architecture and consider expanding the web-based technology implementation throughout the agency. Consideration will be given to expanding the web-based infrastructure systems to respond to the current and future needs for more web-base applications. If a need is identified, plans will be developed to design and implement a new architecture.

3.2.2 Fiscal Year 2002

Growth Management Plan Implementation: This program will implement the Growth Management Plan developed as a result of the Fiscal Year 2001 Growth Management Study.

TWFN Recabling: This program will support the re-cabling of the Two White Flint building at NRC headquarters.

Voice and Data Network Consolidation: This program will implement the voice and data consolidation recommendations developed as a result of the Fiscal Year 2001 study.

3.2.3 Fiscal Year 2003

Fiber to Desktop Study: This program will evaluate the new technologies that provide fiber to the desktop and determine if this technology has any applicability to NRC's needs. The program will use information from the capacity planning activities to determine and forecast the bandwidth requirements for desktop systems, and evaluate the usefulness of installing a pilot fiber to desktop implementation in an office area that has a high bandwidth demand.

Interactive Archive and Retrieval System Study: This program will evaluate the potential methods and systems that may provide a user-controlled interactive file archiving and retrieval system. The system would provide storage for infrequently used files on less expensive media that is easily accessible and can be moved to higher speed direct access storage on request.

Peer-to-Peer Study: This program will evaluate the work-flow and traffic patterns of file and data transfer within the agency to determine if any efficiencies can be gained by providing peer-to-peer architecture.

Workgroup Architecture Study: This program will evaluate the potential technologies that may provide workgroup capabilities at the agency and determine whether these will improve office work flow for any agency processes or groups. If workgroup architecture will improve productivity at the agency, a workgroup architecture that integrates with the existing infrastructure systems will be designed.

3.3.4 Fiscal Year 2004

No programs.

4.0 Hardware Refresh Programs

4.1 Description

These programs provide for a periodic technology refresh of NRC hardware systems at pre-determined intervals. A refresh program can be initiated based on agency needs, as required for continued maintainability, or in response to increasing capacity demands.

4.2 Programs

4.2.1 Fiscal Year 2001

Desktop Monitor Refresh: 19" monitors will be installed on agency desktop systems as funding permits. This program is continued from Fiscal Year 2000.

Desktop PC Refresh: This program will continue to replace agency desktop computer hardware and software as required to maintain efficient and effective operations.

Network Printer Refresh: This program will replace the network printers located in the office areas in the agency. The current printers are expected to be at the end of their useful life in fiscal year 2001.

Network Switch / Router Refresh: This program will replace and upgrade the network switches and / or routers as required to maintain efficient and effective infrastructure operation.

Server Refresh: This program will continue to upgrade or replace the agency network, E-Mail, and web server hardware and software as required to maintain efficient and effective infrastructure operation.

Storage Media Expansion: This program will increase the data storage capacity in response to the increasing demand for electronically stored information. A study will be done to evaluate the advantages and disadvantages of server versus local storage system upgrades. The best value combined systems solution will be selected and implemented. Consideration will be given to the implementation of CD jukeboxes at the servers and local CD readers on desktop PC's. Also, various local (desktop) removable media solutions will be considered for potential implementation, such as jazz and zip drives, recordable CD systems, and tape systems. The implementation of a user-accessible and centralized archive and retrieval system will also be considered.

4.2.2 Fiscal Year 2002

Broadband Video (HQ) Refresh: This program will replace the obsolete broadband head-end closed-circuit broadcast system used to transmit the television cable channels to monitors throughout the headquarters facility. It is expected to have reached the end of its useful life in Fiscal Year 2002. The current system has been out of production for several years and parts are becoming more scarce. This upgrade will expand the capacity and capabilities of the system in order to take advantage of more broadcast, cable and satellite network feeds beyond

those available through Cable TV Montgomery. If necessary, the TV monitors on each floor will be replaced at the same time.

Data Center Printer Refresh: This program will replace the Data Center printers used in production operations. These are expected to be at the end of their useful life in Fiscal Year 2002.

Desktop PC Refresh: This program will continue to replace agency desktop computer hardware and software as required to maintain efficient and effective operations.

Expanded Bandwidth to Desktop: This program will provide higher bandwidth capacity to the desktop in response to increasing network capacity demands and to support the agency's new technology requirements such as desktop video, ADAMS, and multi-media. Implementation may require an upgrade of desktop system Network Interface Cards, network client software, cabling, and network systems as appropriate.

Network Switch / Router Refresh: This program will replace and upgrade the network switches and / or routers as necessary. This refresh will provide greater network capacity, updated technology with improved supportability and maintainability, and support for the expanded bandwidth to the desktop.

Server Refresh: This program will continue to upgrade or replace the agency network, E-Mail, and web server hardware and software as required to maintain efficient and effective operations.

Voice Mail (HQ) Refresh: This program will replace the Octel voice mail system at NRC headquarters. It is expected to have reached the end of its useful life in Fiscal Year 2002.

4.2.3 Fiscal Year 2003

Desktop PC Refresh: This program will continue to replace agency desktop computer hardware and software as required to maintain efficient and effective operations.

Expanded Bandwidth to Desktop: This is a continuation of the program begun in Fiscal Year 2001.

Network Switch / Router Refresh: This program will replace and upgrade the network switches and / or routers as necessary. This refresh will provide greater network capacity, updated technology with improved supportability and maintainability, and support for the expanded bandwidth to the desktop.

Security System/Firewall Refresh: This program will replace the headquarters security systems, such as proxy servers, bastion hosts, and firewall systems. These systems are expected to be obsolete in Fiscal Year 2003 and in need of upgrade to keep pace with security advances in the industry and mitigate potential new technological threats to the agency network.

Server Refresh: This program will continue to upgrade or replace the agency network, E-Mail, and web server hardware and software as required to maintain efficient and effective operations.

4.2.4 Fiscal Year 2004

Desktop PC Refresh: This program will continue to refresh desktop systems at the rate determined by agency requirements.

Network Switch / Router Refresh: This program will replace and upgrade the network switches and / or routers as necessary. This refresh will provide greater network capacity, updated technology with improved supportability and maintainability, and support for the expanded bandwidth to the desktop.

Server Refresh: This program will continue to upgrade or replace the agency network, E-Mail, and web server hardware and software as required to maintain efficient and effective operations.

5.0 Security Programs

5.1 Description

The Security programs provide security for all IT infrastructure systems. Security includes systems that provide account management (user ID and passwords), file, network, application, and data base access. It also provides software for overall network security as well as secure E-commerce capabilities in a web environment.

5.2 Programs

5.2.1 Fiscal Year 2001

Audit Trail and Alert Enhancement: This program will provide new systems and software to record and monitor NRC network and system activities, and provide alerts when suspicious activity is detected. It is intended to improve the audit trail capabilities on NRC systems.

Digital Certificates Capability: This program will expand the capability to issue and recognize certificates guaranteeing the identity of a network component. This technology allows the agency to authenticate the originating system for electronically transmitted data.

Digital Signatures Capability: This program will expand the capability to establish and authenticate the originating party of a message or other information electronically transmitted by and to the NRC. This technology allows the agency to confirm and validate receipt of messages, contracts, purchase orders and all electronic documentation on the agency network.

Enhanced Public Access: This program will expand the capabilities of NRC's external web hosts and associated security systems to allow the public to have online access to more information from the NRC. The agency will consider the implementation of more than one level of access privileges from the public domain, providing different levels of access for public, client and government users.

Network Security Enhancement: This program will implement the recommended changes identified in the Network Security Study conducted in Fiscal Year 2000.

Network Security Study: This program will evaluate the current security systems and determine what changes, if any, need to be made to take advantage of newer security capabilities available from commercial vendors that respond to recent cyber attacks and threats.

Presidential Decision Directive 63 (PDD 63) Study: This program will study and recommend the appropriate agency response to PDD 63, which requires each agency to plan for disaster recovery of IT operations necessitated by hardware failure, security compromise, data losses, or unforeseen events of any type or magnitude. The PDD 63 study will develop a plan for establishing the necessary NRC directives, recovery guidance, and recovery operations to respond to the requirements of PDD 63.

Presidential Decision Directive 63 (PDD 63) Implementation: This program will implement any plans that were made as a result of the PDD 63 study conducted in Fiscal Year 2000.

5.2.2 Fiscal Year 2002

Receipt Authentication: This program will expand the agency's capability to identiFiscal Year the receipt date and time, as well as the identity of the recipient of sent messages and data.

Security System Study: This program will evaluate the current security systems and determine what changes, if any, need to be made to take advantage of newer security capabilities available from commercial vendors that respond to recent cyber attacks and threats. Plans will be made for implementation in Fiscal Year 2003.

Windows 2000 Professional: This program will upgrade the agency desktop systems to the most recent Microsoft Windows operating system release. It will ensure that agency end-users have the latest operating system for functionality; in particular, the security, reliability, performance and interoperability features required to support the programmatic and business needs of the agency. It allows the agency to take advantage of new software that will help it conduct its business by providing the operating environment that is most likely to be used to provide proper performance and maintenance of new commercial software.

Windows 2000 Server: This program will install Microsoft Windows 2000 Server to take advantage of the new security capabilities, new features, and remain current with application development environments.

5.2.3 Fiscal Year 2003

Next Generation Security Systems: As security becomes more and more important, particularly in web-based systems, the expectation is that by Fiscal Year 2003 there will be a next generation of security systems with significant improvements that will replace the current technology. NRC will continue to review and implement the highest level of security that is reasonable and necessary for protection of its systems. This program will design, procure, and implement the new technology, particularly software, that represents the state-of-the-art in security for enterprise systems.

5.2.4 Fiscal Year 2004

No programs.

6.0 Customer Relationship Management Programs

6.1 Description

The Customer Relationship Management programs provide a continuing focus on enhancing and improving the relationship between ITID and it customers in the agency. The emphasis in these programs is on improving communications, establishing service level requirements and agreements, periodically reviewing these items and revising them as appropriate. ITID continues to strive to meet customer requirements for infrastructure services to augment and facilitate the agency's achievement of its mission and objectives. Maintaining open lines of communication and continually monitoring the customers' experience with existing services as well as changes in the customers' services requirements are the primary objectives of the Customer Relationship Management programs.

6.2 Programs

6.2.1 Fiscal Year 2001

Agency Document Access and Management System (ADAMS) Public Access Support: This program will provide extra support to the general public in accessing ADAMS via the external web site. Customer issues in accessing this site will be addressed continuously as they arise until support requirements for public access become predictable and can be reduced to routine agency support procedures and practices.

Baseline Architecture: This program will gather information in order to establish a baseline hardware and software architecture for all ITID systems. This information will eventually be used for input to a configuration management system.

Coordinate / Control Changes: This program will implement a program to coordinate and control changes that are visible to the customers. As part of the Release Management process, it will provide controls and track information about new releases of software and hardware to server and desktop systems. It will ensure that changes are thoroughly tested and integrated and coordinate new releases so that they can be packaged into a single release per month except in emergencies.

Knowledge Tools: This program will implement a method for generating a knowledge data base with useful and current information for support personnel and customers through the use of knowledge tools. This information would be used to expedite the closure of problems reported to the Customer Support Center. Initially the knowledge data base will be implemented for the use of Customer Support personnel, and eventually made available to customers via the Web-based customer support system.

Market Services / Capabilities: This program will establish a method for advertising and promoting ITID's services and capabilities. The agency offices will be informed about what services are available through ITID in order to be better able to consider and take advantage of the efficiencies that can be gained by the use of the agency's automated services. As part of

this program, ITID will prepare orientation materials for new employees and make training materials available to the agency's personnel through the infrastructure systems.

Revise SLR's / SLA's: This program will revise the Service Level Requirements and Service Level Agreements established in Fiscal Year 2000 as required.

Web-based Support: This program will plan, design, and implement a Web-based customer support system for customers to directly access Frequently Asked Questions (FAQ's) regarding NRC's OCIO systems. This system will also eventually be used to provide a front-end for customers to access the Knowledge Tools that will be implemented in the future.

6.2.2 Fiscal Year 2002

Revise SLR's / SLA's: This program will revise the Service Level Requirements and Service Level Agreements established in Fiscal Year 2001 as required.

6.2.3 Fiscal Year 2003

Revise SLR's / SLA's: This program will revise the Service Level Requirements and Service Level Agreements established in Fiscal Year 2002 as required.

6.2.4 Fiscal Year 2004

Revise SLR's / SLA's: This program will revise the Service Level Requirements and Service Level Agreements established in Fiscal Year 2003 as required.

7.0 Office Function Programs

7.1 Description

The Office Function programs provide the planning support and programmatic implementation support required to conduct for enhancements, software improvements, and the overall IT expansion strategies that will provide direct IT support to the desktop. These programs enhance personnel productivity through direct implementation.

7.2 Programs

7.2.1 Fiscal Year 2001

Alternative Desktop Workstation Strategies: This program will consider acceptable alternatives to the standard desktop PC that could be used to support special business needs. Examples of alternative desktop strategies are: 1) Use lap-top PC's as standard desktop systems and provide docking stations for the lap-top PC's in place of the current desktop systems, 2) Augment the standard desktop PC with an interface for a lap-top PC that would allow data to be exchanged between the two systems, and 3) Use thin clients as standard desktop systems. This program will define the standards and implementation strategy and policies for alternative agency desktop systems.

Desktop Video: This program will study and evaluate the business requirements for desktop video. If agency requirements are identified, alternatives will be considered for adding the infrastructure systems necessary to provide the capability of transmitting and receiving video at the desktop PC. Desktop video will allow agency personnel with the appropriate installed desktop equipment and software to attend video teleconferences and view transmissions from their desktop PC's, reducing the need for travel to remote sites, and eliminating the need to use a video conference room. Associated with this is a study of whether to continue with and implement into full production the technology used in the StreamPipe.Com pilot conducted in FY 2000. StreamPipe provided Internet-based video broadcast of commission hearings to the general public.

Effective Use of Automation Tools: This program will identify operational process changes that could be made to take advantage of the new IT support automation tools that are on the market in Fiscal Year 2000/2001 for improving efficiency and effectiveness in IT operations. The new Help Desk system will be evaluated as a possible vehicle for automating some processes. As part of this effort, a Network Tools Plan (NTP) will be developed and maintained. Some additional new automation tools may be purchased and installed as part of this program.

E-Mail Upgrade - Novell GroupWise 5.5: This program will upgrade the E-Mail system software on desktops and servers to Novell GroupWise 5.5. The upgrade will provide recent maintenance software improvements, including better application integration and interoperability and more efficient system operation.

Video Expansion: This program will acquire and install additional video teleconferencing (VTC) units for agencywide video teleconferencing at Region III and the headquarters auditorium to support the growing agency demand for teleconferencing facilities.

Work From Home Program Upgrade: This program will address the user issues related to the Work From Home Program at the agency. Preliminary feedback from users indicates that the response time when using certain applications from home or while on travel needs to be improved. This will require further analysis to determine whether this is common to all users or affects only a few users. The program will identify any new agencywide requirements, research the available technologies for satisfying these requirements, and identify any solutions that can be implemented in Fiscal Year 2001 within the agency's budget constraints.

7.2.2 Fiscal Year 2002

Browser Refresh: This program will install new browser software on the desktop systems at the agency. Web information presentation software is constantly changing and a browser refresh will be necessary to ensure the information that is provided on the web continues to be accessible using the new web technologies.

Conference Room Workstations: This program will provide workstations in the conference rooms at headquarters. These workstations will provide attendees with access to the network systems during meetings.

E-Mail Refresh: This program will replace/upgrade the NRC E-Mail system to one that is compatible with the new Office Suite (see below) and that can support the agency into the next millennium.

Multi-Media Capability at Desktop: This program will provide multi-media capability at desktop PC's if new agency requirements for this capability are identified in Fiscal Year 2001 and the investment has been justified.

Office Suite Refresh: This program will upgrade all agency desktop systems to a new standard Office Suite and upgrade or install other additional office software programs as required to augment the suite. The upgrade will provide a current, manufacturer-supported suite of office products for agency programmatic and business use. Selection and timing of this upgrade will be determined by the results of the Office Suite Study conducted in Fiscal Year 2000.

Portable Communications Services (PCS): This program will identify any new or increasing agency requirements for portable technologies suitable for incorporation into the NRC environment such as: programmable pagers and cellular phones, radios, portable computing devices, personal digital assistants (PDA) and Palmtop computing devices. If a need is identified, standard products will be selected and standard configurations will be developed for implementation throughout the agency. This program will purchase units and provide NRC network connections and supporting software as required.

Wireless Office: This program will evaluate the potential benefit, technical feasibility, and security risk of allowing agency personnel to use wireless technology for data or voice

communications with agency systems. A feasibility study and requirements analysis will be conducted.

7.2.3 Fiscal Year 2003

Agencywide Desktop Video Study: This program will evaluate the agency experience with desktop video to date and consider the benefits of expanding the desktop video implementation agencywide. Expansion could potentially reduce the video teleconferencing services requirements in NRC meeting rooms.

Agencywide Multi-Media Study: This program will evaluate the agency experience with the multi-media capabilities at the desktop to date and consider the benefits of expanding the capability agencywide.

Voice Mail Notification via E-Mail: This program will study the need for and implement as required an interface between the voice mail system and the E-Mail system at headquarters. With such a capability, when voice mail messages are recorded on a user's telephone voice mailbox, the voice mail system would automatically notify the recipient that a message is waiting, via a message in the inbox on their E-Mail system. This is an automated implementation of the "universal mailbox" concept. When fully implemented, "universal mailbox" allows a user to see at a glance all incoming communications, regardless of the origin or medium used for storage. Other potential future implementations of the "universal mailbox" at the agency might include automatic notification of incoming AUTODIN, facsimile and Telex communications, as the technology becomes available.

7.2.4 Fiscal Year 2004

No programs.

8.0 Business Application Infrastructure Programs

8.1 Description

The Business Application Infrastructure programs support the development of the IT infrastructure platforms that are configured to meet business applications requirements. Included are web-based special workstation environments that will meet the needs of the disabled worker. Also included are web-based application platforms.

8.2 Programs

8.2.1 Fiscal Year 2001

Agencywide Documents Access and Management System (ADAMS) Transition to Full Production Support: This program will develop and implement a plan to transition ADAMS from development to an ongoing production operations mode. This program will establish plans and procedures for ADAMs updates and upgrades to agency servers, workstations, and websites as prescribed by the overall ADAMS development schedule. In Fiscal Year 2001, one ADAMS update will be completed.

Application Architecture: This program will plan and design an architecture for the IT infrastructure to support multiple, agencywide client/server applications. The intent of this program is to provide a versatile, general purpose environment that accommodates the needs of most applications developers and eliminates the need to build and maintain custom environments for individual agencywide applications. The goal of this program is to enable all applications to run on a common platform and co-exist with other applications.

Data Warehousing Pilot: This program will conduct a data warehousing pilot project to develop a proof of concept system and evaluate the utility to the NRC.

Disability Assistance: This program will investigate and plan for the development and implementation of technologies designed to maximize the contributions and productivity of handicapped and visually impaired employees. The Disability Assistance program responds to the requirements of the Americans with Disabilities Act.

Electronic Information Exchange (EIE) Pilot: This program will assess the capabilities and technologies available for processing electronic communications and performing data transfer between multiple and unrelated software and computer platforms. A pilot will be conducted with another enterprise during Fiscal Year 2000 to test the feasibility of this capability.

Electronic Information Exchange (EIE) Production: This program will develop and implement a production EIE solution based on the results of the Fiscal Year 2000 pilot, assuming that it was successful.

Starfire Time and Labor Pilot Support: This program will develop and implement a plan to continue to support the Office of the Chief Finanancial Officer (OCFO) in its pilot of the Starfire Time and Labor Reporting application. Support for this pilot will include testing, integration into

the Production Operations Environment (POE), the necessary POE upgrades, new operational procedures and activities, and help desk support services.

Starfire Time and Labor Support Plan: This program will coordinate with the OCFO and Human Resources to develop and implement a plan to transition the Starfire Time and Labor Reporting application from a development pilot to agencywide production operations mode. This program will establish plans, procedures and schedules for roll-out of the Starfire application to infrastructure servers and workstations as prescribed by the overall Starfire development schedule. In Fiscal Year 2001, testing of production operations support functions is expected to begin, help desk support personnel will be trained, and ITID will integrate, install, test, operate and maintain the server and client environments for the application.

8.2.2 Fiscal Year 2002

ADAMS Refresh: This program will upgrade or replace the hardware and software systems associated with the Agency Document Access and Management System (ADAMS) application. New components will be installed to respond to increased usage and capacity requirements or other quality of service issues, such as obsolete hardware and software.

E-Commerce: This program will implement and support agencywide applications that use Electronic Commerce capabilities.

Data Warehousing Implementation: This program will implement a Data Warehousing application based on the results of the pilot conducted in Fiscal Year 2001. The Fiscal Year 2002 schedule for implementation into the agency production operations environment, is contingent on the successful completion of the "proof of concept" pilot by the end of Fiscal Year 2001.

Starfire Time and Labor Application Transition to Full Production: This program will support the transition of the Starfire Time and Labor Application to full production.

Voice Recognition System: This program will implement a voice recognition system to be used for data entry and interaction with PC's. This system will operate as an alternative to the keyboard and mouse, and will support the disability assistance program.

Web Architecture Implementation: This program will use the results of the Web Architecture Study (see 3.0 Capacity Planning Programs) to design, procure, and implement the architecture and systems needed to create an infrastructure capable of supporting future web applications.

8.2.3 Fiscal Year 2003

ADAMS Refresh: This program will upgrade or replace the hardware and software systems associated with the Agency Document Access and Management System (ADAMS) application. New components will be installed to respond to increased usage and capacity requirements or other quality of service issues, such as obsolete hardware and software.

Commercial TV Channel Capacity Expansion: This program will evaluate the possibility and need for expanding the capacity of the NRC headquarters in-house broadcast system to provide additional networks and channels, including those available via commercial cable networks, commercial satellite networks, and Internet broadcast service providers.

8.2.4 Fiscal Year 2004

ADAMS Refresh: This program will upgrade or replace the hardware and software systems associated with the Agency Document Access and Management System (ADAMS) application. New components will be installed to respond to increased usage and capacity requirements or other quality of service issues, such as obsolete hardware and software.

9.0 Management and Administration Programs

9.1 Description

Management and Administration programs support the planning activities needed to ensure that a robust IT environment capable of exceeding established requirements of NRC users is acquired for the lowest overall cost of operation.

9.2 Programs

9.2.1 Fiscal Year 2001

Account Management Consolidation: This program will study, make recommendations, and implement system and process changes as required to consolidate and centralize the assignment of computer system accounts, User ID's, and passwords for all systems used by personnel at the agency.

Infrastructure Development Plan: This program will provide planning, development, design and technical support for the evolving infrastructure systems requirements.

Infrastructure Services and Support Contract (ISSC): This program will provide planning and support for the development of statements of work, delivery orders, task orders, and source selection activities. The program will also provide transition, migration, and implementation support of the task orders or contracts that will replace several ITID services and support contracts in Fiscal Year 2001 and Fiscal Year 2002, including the Next Generation Network contract and the Telecommunications Support Services contract.

Maintenance Cost Model: This program will develop a maintenance cost model and define a process for weekly maintenance reporting. The goal of this program is to provide hardware cost of ownership comparisons based on the maintenance and upgrade history in order to determine which computer equipment has the lowest annual maintenance cost and to identify when it would be less costly to replace instead of maintain a given type of equipment. This information can also be used to identify trends and high failure rates which will provide information for agency decisions on whether to initiate agencywide preventive maintenance actions.

Operating Plan: This program will provide the annual Operating Plan for ITID, which contains a summary of the ITID programs for the Executive Director for Operations.

Personal Computing Policies and Procedures: This program will develop procedures for procurement, distribution, maintenance, and inventory tracking of personal computing devices provided to agency personnel such as laptops, Palm Pilots™, personal assistants, etc.

Presidential Decision Directive 67 (PDD 67): This program will develop a plan to provide continuity of agency operations in a degraded environment caused by a variety of natural disasters and unforeseen events. PDD 67 planning provides the agency guidance and procedures needed to establish the inter-agency agreements needed to continue day-to-day business operation of the NRC under such circumstances.

Records Management: This program will provide support for the agency's record management activities, including document management, ADAMS support, and the requirements of the National Archives and Records Administration (NARA).

Strategic Plan: This program will provide the annual planning required to align the business activities of ITID with the business objectives of the agency as a whole. The Strategic Plan provides the programmatic and budgetary frameworks for ITID to meet agency expectations.

Technical Reference Model (TRM): This program will evaluate and select new target standards for the agency that reflect the current and future IT technologies used by NRC. The standards will be documented in the agency's Technical Reference Model (TRM). This model provides guidance to the development organizations and NRC offices to be used in their future IT development and procurement plans. Agencywide adherence to the guidance provided in the TRM is essential to continue to maximize the performance, maintainability, interoperability, scalability, and portability of current and planned hardware and software systems within the NRC.

WITS/FTS Transition: This program will provide the comprehensive planning and support needed to conduct the transition, migration, and implementation of new telecommunications services contracts. These new contracts will replace the expiring Washington Interagency Telecommunications Services (WITS) (Bell Atlantic), and Federal Telecommunications Services 2000 (FTS2000) (AT&T) contracts that the agency has used for several years. The General Services Administration (GSA), which awarded and administers the WITS and FTS 2000 contracts, has awarded replacement contracts which could potentially be used by the agency.

9.2.2 Fiscal Years 2002/2003/2004

Infrastructure Development Planning: This program is continued from Fiscal Year 2001. See Fiscal Year 2001 for a description.

Infrastructure Services and Support Contract (ISSC): This program will provide management, administration, independent validation and verification of deliverables, independent performance measurements, and on-going oversight of invoices for the ISSC contract.

Strategic Plan: This program is continued from Fiscal Year 2001. See Fiscal Year 2001 for a description.

Operating Plan: This program is continued from Fiscal Year 2001. See Fiscal Year 2001 for a description.

Technical Reference Model (TRM): This program is continued from Fiscal Year 2001. See Fiscal Year 2001 for a description.

INFRASTRUCTURE DEVELOP' ˜NT FORECAST-AT-A-GLANCE

INFORMATION TECHNOLOGY INFRASTRUCTURE DIVISION
Development Forecast, Fiscal Years 2001 - 2004
SUBJECT INDEX

Subject **Page**

Account Management Consolidation 22
ADAMS 14, 19-21
Agency Document Access and Management System (ADAMS) Public Acce 14
Agencywide
- client/server applications 19
- Desktop Video Study 18
- Documents Access and Management System (ADAMS) Transition to Ful 19
- Multi-media Study 18
- Video Expansion 17
- Work From Home 17

Alternative Desktop Strategies 16
Application Architecture 19
Application Standardization 5
Architecture
- Application 19
- Baseline 14

Audit Trail and Alert Enhancement 12
Automation Tools 16
Back-up System Consolidation Strategy and Implementation 3
Baseline Architecture 14
Benchmarking 7
Broadband 17
Business Application Infrastructure Programs 19
Business Continuity Planning 3, 4
Capacity Planning Programs 7
Changes
- Control 14
- Coordinate 14

Commercial TV Channel Capacity Expansion 20
Conference Room Workstations 17
Customer Newsletter 14
Customer Relationship Management Programs 14
customer support
- Frequently Asked Questions 15
- Knowledge Tools 14
- Market Services / Capabilities 15
- Meetings with Regions 15
- Newsletter 14
- Public Access 14
- SLR's / SLA's 14, 15
- Web-based 15

Data Warehousing

INFORMATION TECHNOLOGY INFRASTRUCTURE DIVISION
Development Forecast, Fiscal Years 2001 - 2004
SUBJECT INDEX

Subject **Page**

Implementation 20
Pilot 19
Desktop Monitor Refresh 9
Desktop PC Refresh 9, 10
Desktop Strategies 16
Desktop Video 17
Desktop Video Study 18
Digital Certificates Capability 12
Digital Signatures Capability 12
Disability Assistance 19
E-Commerce 20
E-Mail
Refresh 17
Upgrade - Novell GroupWise 5.5 16
Voice Mail Notification 18
Electronic Information Exchange (EIE)
Pilot 19
Production 19
Expanded Bandwidth to Desktop 10
Fiber to Desktop Study 8
FTS2000 23
Growth Management Plan Implementation 8
Growth Management Study 7
Hardware Refresh Programs 9
Help Desk System Refresh 3
Infrastructure Development Planning 22
Infrastructure Development Process Model (IDPM) 5
Infrastructure Services and Support Contract (ISSC) 22
Integrated Network Management System (INMS) Enhancements 4
Integration of VTC, Broadband, & Desktop Video 17
Interactive Archive and Retrieval System Study 8
laptop 18
Maintenance Cost Model 22
Management and Administration Programs 22
Meetings with Regions 15
Mobile Office 18
Multi-media at Desktop 17
NetWare Over IP 5
NetWare V5 4
Network Printer Refresh 9
Network Security Enhancement 12
Network Security Review 12

INFORMATION TECHNOLOGY INFRASTRUCTURE DIVISION
Development Forecast, Fiscal Years 2001 - 2004
SUBJECT INDEX

Subject **Page**

Network Server and Web Server Refresh 9, 10
Network Switch / Router Refresh 9, 10
Newsletter 14
Next Generation Security Systems 13
Office Function Programs 16
Office Suite Refresh 17
Operating Plan 22, 23
Operations and Maintenance Programs 3
Palm device 18
Peer-to-Peer Study 8
Personal Computing Policies and Procedures 22
Personal Digital Assistance (PDA) 18
Presidential Decision Directive 63 (PDD 63) Implementation 12
Presidential Decision Directive 63 (PDD 63) Study 12
Presidential Decision Directive 67 (PDD 67) 23
Production EIE 19
Production Operations Management 5
Production Test Lab 5
Public Access 12, 14
Receipt Authentication 13
Records Management 23
Refresh
- Bandwidth 10
- Desktop 10, 11
- Desktop Monitor 9
- Desktop PC 9
- Network Printer 9
- Network Server 9-11
- Network Switch 9, 11
- Office Suite 17
- Router 10, 11
- Security System/Firewall 11
- Storage Media 9
- Voice Mail (HQ) 10
- Work From Home Program 17

Release Management 6
Remote Access Upgrade 17
Remote Keyboard, Display, and Monitor for Remote Server Operatio 4
Router 10
Security Programs 12
Security System Study 13
Security Systems 13

INFORMATION TECHNOLOGY INFRASTRUCTURE DIVISION
Development Forecast, Fiscal Years 2001 - 2004
SUBJECT INDEX

Subject **Page**

Audit Trail and Alert 12
Digital Certificates 12
Digital Signatures 12
Enhancement 12
Next Generation 13
PDD 63 12
Refresh 10
Review 12
Study 13
Service Level Agreements 14
Service Level Requirements 14
SLR 14
Smartphone 18
Software Suite Study 17
Standardization Programs 5
Starfire Time and Labor
Pilot Support 19
Roll-out to Infrastructure Systems 20
Transition to Full Production 20
Storage Media Expansion 9
Strategic Plan 23
Technical Reference Model (TRM) 22, 23
TV Channel 20
TWFN Recabling 8
Video 17
Video / Data Network Consolidation (Video over IP) 6
Video Expansion 17
Voice and Data Network Consolidation 8
Voice and Data Network Consolidation Study 7
Voice Mail (HQ) Refresh 10
Voice Mail Notification via E-Mail 18
Voice Recognition System 20
VTC 17
Web Application Infrastructure 20
Web Architecture Study 8
Windows 2000 Professional 13
Windows 2000 Server 13
wireless 18
Wireless Office 18
WITS/FTS Transition 23
Work From Home Program Upgrade 17
Workgroup Architecture Study 8

SUBJECT INDEX

Subject **Page**