Contract Line Item Number 0003

INFORMATION TECHNOLOGY SERVICES IN SUPPORT OF THE NATIONAL NUCLEAR SECURITY ADMINISTRATION (NNSA) PROGRAM MANAGED BY BWXT Y-12

CONTENTS

APPENDICES

1. PURPOSE

This segment of the Performance Work Statement (PWS) defines requirements for information technology (IT) services in support of the (DOE's)/National Nuclear Security Administration's (NNSA's) Y-12 National Security Complex located in Oak Ridge, Tennessee. IT services to be provided include applications software development and maintenance, desktop support services, computer resources operations and management, network and voice communications administration, and general IT support services.

2. BACKGROUND

Y-12 National Security Complex

The national security mission in Oak Ridge is carried out at the Y-12 National Security Complex, formerly known as the Oak Ridge Y-12 Plant. Programs at Y-12 National Security Complex include: manufacturing and reworking nuclear weapon components; dismantling nuclear weapon components returned from the national arsenal; serving as the nation's safe, secure storehouse of special nuclear materials; quality evaluation and surveillance of the nation's nuclear weapon stockpile; and support to DOE, other federal agencies, and other national priorities. Y-12 National Security Complex, which employs approximately 4800 employees, is operated by BWXT Y-12 for the NNSA.

A DOE Q-clearance shall be required for Contractor employee(s) who may be needed for on-site support within the Protected Area of the Y-12 National Security Complex. All others shall be required to have at least an L-clearance if entry in the Limited Area of the Y-12 National Security Complex is required.

3. SCOPE OF WORK

3.1. Overview

The Contractor shall provide enterprise information planning and management and assistance in development of architectures, standards, IT management and operations processes, organizational structures, and implementation plans or roadmaps.

The Contractor's process, procedure, and methodology framework should have a solid foundation and be derived from a reputable industry standard, such as Information Technology Infrastructure Library (ITIL).

The Contractor shall:

1. adhere to enterprise-level IT architectures and standards,

2. assist in evaluating technical direction within the context of these architectures and standards, and

3. make recommendations to the Chief Information Officer (CIO) concerning:

    - infrastructure improvements,
    - process improvements,
    - architectures and standards improvements, and

- new technologies that would reduce operational costs and/or significantly improve the level of service.

IT resources managed within the PWS are generally available for use 24 hours a day/7 days a week, excluding approved, scheduled outages and unscheduled outages beyond the control of the Contractor. It is expected that such general availability of networks, servers, and production applications shall continue. These resources are noted in Appendix C-1 BWXT Y-12 Computer Equipment List.

3.2. Task Descriptions

3.2.1 Unclassified Desktop Support Services

3.2.1.1 Introduction

The Contractor shall provide desktop support services for the Y-12 National Security Complex, including computing access management, Internet and intranet information support, virus removal/cleanup, field support, and related services

The Y-12 National Security Complex has approximately 4200 desktop users holding almost 5500 user IDs including Y-12, NNSA Area Office and Wackenhut Services. There are approximately 25 Macintosh personal computers (PCs) in the Y-12 National Security Complex.

In the Unclassified National Security Related (UNSR) environment, there are up to 1000 user accounts, including up to 1000 e-mail users.

Planning is currently underway to standardize on Windows XP PC desktops with a standard base software configuration and support model that includes network delivery of software tools and applications including Office 2002/2003, software upgrades, and central server file space with nightly backups.

IBM Tivoli endpoint software (Contractor furnished) is currently installed on most unclassified PC desktop machines and is utilized for hardware and software inventories, remote assistance, and network access.

The list of software supported for the Y-12 National Security Complex includes Commercial Off-The-Shelf (COTS) packages, desktop operating systems and communications protocols, and local applications as shown in Table 1. Table 2 identifies optional software packages that may be ordered over the network. Table 3 indicates the current standard desktop hardware configurations for purchases made by the Y-12 National Security Complex.

Table 1. Supported desktop software

- Windows 2000 and Windows XP
- Windows Dial-up Networking [point-to-point protocol (PPP)
- VPN client support: 5.1.7 3DES for Windows 2000; 5.1.10 for Windows XP
- SecureCRT
- SecureFX version 2
- Microsoft Internet Explorer version 5.5 SP2; Internet Explorer 6.0 with no customization
- Adobe Acrobat Reader 4.0 or higher and MLP 3.01 or higher
- Adobe Acrobat Exchange version 4.0, 5.05, or higher (troubleshooting with regard to installation, printing, and execution error messaging; not installation)
- Aladdin Expander/Stuffit Expander 5.0 for PC
- McAfee VirusScan 4.03, 4.5; 4.5.1 for XP systems
- MS Office 2002/2003 Pro (includes Word, Excel, PowerPoint, Access, and MS Exchange/Outlook)
- Tivoli endpoint (Contractor furnished)
- Entrust Desktop Suite 6.1 or better
- SAP Client 6.2

For the following locally developed applications, support is for installation and desktop technology support.

- Universal Computer Access Management System (UCAMS)
- WebWHOS (online employee directory information)
- Software Product Update Distribution Service (SPUDS)

Table 2. Optional desktop software

The following software shall be available from purchase directly from the Software Product Update and Distribution System (SPUDS) (with SPUDS retaining software license evidence).

- MS Project 2002 or higher
- Visio 2002 Professional or higher

Table 3. Standard Desktop Hardware Configuration

The following hardware configurations are currently the standard for new purchases. Desktop: Dell Optiplex 2.8 GHz 512 MB memory 40 GB hard disk CD-RW (1) 17-in. SVGA monitor Ethernet board/NDIS Laptop: Dell Latitude D600, 1.6GHz, Pentium 4, 512MB, DDR SDRAM, 32MB NV17, DDR Nvidia Video Card 30GB Hard Drive, Windows XP, Internal 8-24-10-24xSWDVD/CDRWcombo Printers: Network: HP 2300dtn for black/white and the HP 4600dn or Okidata C5300n for color Desktop: Okidata B4300n Facsimile: Hewlett Packard FAX 1230XI

3.2.1.2 Services

3.2.1.2.1 Universal Computer Access Management System (UCAMS)

The Contractor shall manage and administer user authentication and resource access control over networks and systems. The locally developed Web-based Universal Computer Access Management System (UCAMS) tool shall be used to provide administration of user IDs, passwords, and computing resource authorizations. The current baseline pool of user accounts includes approximately 5500 user IDs. The Contractor shall provide Helpdesk support for UCAMS division coordinators and approvers and general user assistance. This includes use of UCAMS and Windows 2000/2003 Active Directory infrastructure, both of which are supported under this PWS.

3.2.1.2.2 HelpDesk Service

The Contractor shall provide a computer HelpDesk service for information and assistance on computing issues and supported software (see Table 1, Supported Desktop Software), assuming an average of 3000 requests per month.

Full service helpdesk support, augmented by remote assistance capability, is to be provided from 7:30 a.m.–5 p.m., Monday–Friday, excluding holidays, with limited service (status information, account verification, and logging request for next workday service) available at other times. HelpDesk staff shall track requests and respond to service requests as specified in Performance Requirements. Desktop problems shall preferably be accommodated via remote assistance, with alternative consulting support methods used only when remote assistance is not effective.

In the event of a widespread system or service outage, HelpDesk and/or Web support personnel shall broadcast an authorized announcement in a timely manner (via prominent Web notice and/or e-mail to all affected users) explaining the outage, prognosis for solution, and a follow-up announcement when problem is resolved.

3.2.1.2.3 Virus Protection and Cleanup

The Contractor shall provide administrative/HelpDesk support for virus clean-up incidents, as directed by the Information Systems and Technology (IS&T) organization.

Desktop virus problems shall be handled via remote assistance with alternative support methods such as office visits used only when remote assistance is not effective.

The Contractor shall provide administrative planning, additional technical and documentation support, and HelpDesk support for a virus that is deemed to be an 'acute' virus (i.e., those which require an enterprise-wide strategy and significantly more work).

3.2.1.2.4 Software Product Update Delivery System

1. The Contractor shall provide network-based software delivery (currently using the SPUDS application for this function). Support for online ordering, delivery, and management of software over the network includes:

    1.1. Local delivery of supported software (Table 1 with supporting documentation for licensing, installation, and use) and ordering service for other products (Table 2 with no customization and minimal documentation).

    1.2. Ability for users to transfer software they own to another user ID, or to correct information concerning licenses held (e.g., CPU property number).

    Assume the total product list managed through this service is approximately 75 software packages. This activity involves interactions with vendor, procurement, and finance personnel. Software purchased for SPUDS distribution shall be only that software needed for BWXT Y-12 consumption.

2. The Contractor shall provide software license management including:

    - purchasing the pool of available software products for distribution,
    - inventory management,
    - licensing documentation, and
    - software license compliance.

3.2.1.2.5 Desktop Office Visits

The Contractor shall provide office visits when needed to resolve desktop computing software problems.

3.2.1.2.6 Laptop Loaner Pool

The Contractor shall manage approximately 20 laptops in a laptop loaner pool, including support for Web requests of a laptop loaded with standard desktop applications, such as Microsoft Office and e-mail, for a loan period of less than one month. The minimum lead

time for laptop availability is 24 hours from the request date, and the maximum lead time is two (2) weeks. Laptops shall be returned to their original state upon return to the pool.

The Contractor shall maintain an inventory of the hardware and associated software for laptops and provide inventory reports upon request.

3.2.1.2.7 Electronic Mail Services

The Contractor shall provide fully supported electronic mail services, including:

1. account maintenance, e-mail troubleshooting, and data store for Microsoft Exchange/Outlook users,

2. access by desktop Outlook client or Web browser,

3. directory functions that support WebWHOS and enable addressing of BWXT Y-12 user IDs without having to specify the full path or mail server, and

4. central e-mail router for @y12.doe.gov, with propagation of the routing database nightly to NT (Exchange), VMS, and limited UNIX e-mail hosts and servers.

In the UNSR environment, the Contractor shall provide fully supported electronic mail services, including account maintenance, e-mail troubleshooting, and data store for Microsoft Exchange/Outlook users. No access to users outside this UNSR e-mail server is permitted.

3.2.1.2.8 Web Management

The Contractor shall provide:

1. Core Web Content Management**:** Manage and maintain top-level intranet and Internet pages (approximately 90 pages intranet and 50 pages Internet). Convert and post new procedures in the Management Requirements Web area; maintain application that delivers procedures. Convert and post Bechtel job postings to Bechtel “Jobs” Web page. Fine-tune format, convert, and post organization charts to “Org Chart” Web area; maintain application that collects, delivers, and archives organization charts. Maintain Benefit Administration and Benefit Plans Web sites. Maintenance of these sites does not include development of new functionality (i.e., database interaction or completely new sections of Web sites) but can include additional static pages for existing Web areas or sections of Web sites

2. Guidance, instructions, and support for Web page owners and Web users (approximately 60 calls per month): Answer questions, provide guidance, and develop Web instructions in support of information providers and Web users. Track required forms for Web areas; monitor access to Web areas; maintain application (database-driven) that stores information on forms; notify users of required periodic reviews of Web sites and monitor responses to notification. This effort does not include development of new database-driven functionality that might be needed as requirements change.

3. Web-based query and reporting of desktop hardware/software inventory data acquired and managed in this PWS.

4. Web Content Configuration Management: Maintain quality and currency of unclassified intranet and Internet content (information pages). Manage data in accordance with the information placement and maintenance procedure for the unclassified Web environment. Information (consisting of information owner, description, date of last change, etc.) concerning each Web information area is to be entered by the user to a central repository. Configuration of the Web information area is managed by the Contractor as part of the overall Configuration Management process.

5. Online computing information and news articles for local systems and software delivered via the BWXT Y-12 Information Technology Portal, including installation instructions and how-to information, self-help tools (desktop videos, etc.), and tips on using software.

   The schedule for provision of online information and news articles shall be managed by the Contractor, with CTM approval.

   This service includes:

   5.1. maintenance updates of online information for existing systems and products and development of online information for new/upgraded systems and products,

   5.2. updates to previously published computing news articles as necessary.

   Updates to documentation for non-supported products and services are not included in this Service.

6. Management of the BWXT Y-12 unclassified Web servers including:

   6.1. support of https service, assuming software is provided,

   6.2. capability for up to five (5) additional virtual domains for internal and/or external Web servers,

   6.3. full-text search capability, including installation and configuration of upgrades, as well as maintenance of the software tool, UltraSeek, and support for users of the search engine (assume number of user calls shall be approximately ten per month),

   6.4. management of intranet and Internet content and provide indexing capabilities including monitoring of performance and adjustments to index entries as needed for performance (assume approximately 600 entries with more than 90,000 accesses per year),

   6.5. regular load of user-directory information to support WebWHOS service, including pointers to other Online Phone Book (PH) servers and the pager request application (assume approximately six pointers),

   6.6. developer support for server-based tools plus commonly needed functional tools (e.g., inactivity timeout tools, Data Encryption Standard (DES) encryption modules, SAP (Systems, Applications and Products in data processing) cost object validation routines), and

6.7. elimination of banner and/or footer indication of the organization providing the Web hosting service. Only affiliation(s) required by BWXT Y-12 or requested by the page owners shall be displayed.

3.2.1.2.9 Public Key Infrastructure

The Contractor shall:

1. Provide support for Entrust Public Key Infrastructure (PKI) system console functions according to the DOE PKI Certificate Policy and Y-12's Certification Practice Statement (CPS). This support includes configuring DOE Certificate Authority equipment and software, serving as Master Users or First Officers for certain formally defined procedures, and securely managing associated passwords and key tokens.

2. Provide user registration and user support services (i.e. serve as Registration Authorities) for Y-12's Entrust PKI service, including adding new users into the Entrust directory, authenticating user identities face-to-face, assisting users with installation of Entrust desktop software and later troubleshooting problems, etc. Assume thirty new users receive Entrust certificates per month.

3.2.1.3 Performance Requirements

The following response times are required, based on method of request, priority of the request, and method for resolution. Priority is set by the HelpDesk based on Y-12's description of the problem.

1. Initial requests: The Computer HelpDesk shall receive requests via phone, fax, e-mail, and Web submission. HelpDesk shall answer telephone calls 80% of the time with less than a 30-second wait and enter the request into the tracking system. E-mail and fax requests shall be entered into the tracking system within 2 hours of receipt.

2. Response and resolution: The urgency and complexity of a service request affects resolution time. Contractors shall respond 80% of the time to tracking system entries within the time frames as shown in Table 4 and shall immediately initiate work to resolve the request. Regardless of the resolution time required, the CTM shall be kept informed of the progress until the service request is completed. The CTM shall be informed upon completion.

3. Office visits: On occasions when remote services have not been sufficient to resolve problems, the most efficient and least frustrating solution for the Y-12 National Security Complex may be a visit to the Y-12 National Security Complex for problem resolution. If an office visit should be required, the Contractor shall contact the user within four (4) hours to discuss the details and schedule an office visit.

See Table 4 for specific service level priority designations and response times during full-service hours. For each priority level, response time means that the Contractor has initiated work on the request. For priority levels 1–3, problems outstanding (unresolved) after 4 hours shall be escalated for resolution.

Table 4. Service Level Priority Designations

*Priority Level 3—Respond within 15 minutes** • Problem affects large BWXT Y-12 base, or • Problem/request has a critical deadline, or • No alternative method exists to accomplish the Service
*Priority Level 2—Respond within 30 minutes** • Problem affects BWXT Y-12 but work can continue, or • Problem in progress but priority changes due to change in BWXT Y-12 time constraints
*Priority Level 1—Respond within 2 hours** • Problem has little or no impact on continuation of work
*Priority Level 0—Respond within 8 hours** • CTM would like information when possible

*Response time for Desktop User Support Service elements only; the response time for service elements outside this scope and special support services depends on the current volume of requests for services and may not meet these criteria.

3.2.2 Classified Desktop Support Services

3.2.2.1 Introduction

The Contractor shall provide classified desktop support services, including computing access management, user terminal services and thin client support, online computing help and documentation, classified Exchange 2003 services, HelpDesk, classified Windows 2000/2003 active directory support, classified Web servers, classified intranet information support, classified user id and password distribution and administration via classified UCAMS, standard desktop configuration support, support for access to Nuclear Weapons Complex (NWC) connectivity, training and education, and related services to the classified computing environment.

BWXT Y-12 currently supports up to 1000 classified computer users, many of whom have access to classified systems from the shop floor, but are not typical desktop users. Approximately 600 users would be considered administrative/office users. The remaining users require only Computer Access Authorization (CAA) services. There are currently approximately 20 local and 40 remote SecureNet users. The desktop users require support services described in 3.2.1 Unclassified Desktop Support Services. More than 400 of the classified desktops are diskless workstations using terminal services and thin client support.

The goal is to provide classified desktop users with standard software and services based on private and shared disk space with nightly backups, e-mail service, and network delivery of software and Web-based information. In addition, classified users need support for cross-site access as part of the increasingly connected NWC community.

BWXT Y-12 is currently using the SAP portal toolset.

General Note Regarding SecureNet

An important part of support for classified users is connection to the NWC SecureNet. SecureNet is managed outside of the Y-12 National Security Complex for the NNSA NWC facilities as described in Service 3.2.9 Classified Systems Administration, 3.2.9.2 Services, Item 10.

Supported Desktop Software

The list of software supported for the Y-12 National Security Complex includes COTS packages, desktop operating systems and communications protocols, and local applications (for about 300 personal computers) is shown in Table 5.

Table 5. Supported Desktop Software

– Windows 2000, Windows XP – Adobe Acrobat Reader 6.0 and MLP 3.01 – Adobe Acrobat Exchange version 5.05, 6.0 (troubleshooting with regard to installation, printing, execution error messaging; not installation) – MS Office 2002/2003 Pro (includes Word, Excel, PowerPoint, Access, and MS Exchange/Outlook) – McAfee VirusScan 4.5.1	– Microsoft Internet Explorer, v 5.5 Sp 2 and v 6.0 – SecureCRT – SecureFX version 2 – IBM DCE/DFS client – Aladdin Expander/Stuffit Expander 5.0 for PC – Xwin32 X-emulation software – Entrust Desktop Suite 6.1 or better – NetCensus and Server Census version 2.96 – Selected applications: SAP client, Classified UCAMS, Classified WebWHOS

3.2.2.2 Services

The Contractor shall provide server-based computing services, centrally managed application/tool sets, Internet service, and private and shared group disk space for classified desktops. Special provisions are made (as currently defined by classified environment requirements) to maintain secure classified networking services while providing the following:

3.2.2.2.1 Classified Universal Computer Access Management System (UCAMS)

Management and administration of user authentication and resource access control for classified networks and systems, including SecureNet accounts. This includes the use of classified UCAMS and Oak Ridge domain infrastructure, both of which are supported under 3.2.9 Classified System Administration.

3.2.2.2.2 Classified Electronic Mail Services

Support for e-mail services (Classified MS Exchange/Outlook), which includes maintaining accounts, e-mail troubleshooting, data storage, and directory functions that enable addressing classified users by last name or user ID, without having to specify the full path or mail server. A maximum of 1000 e-mail users are to be supported. E-mail directory functions

may be limited to classified Exchange 2003 users and include support of connection to NWC SecureNet.

3.2.2.2.3 Classified Web Management

1. Management of classified intranet content (including pages accessible to remote NWC personnel via Distributed Computing Environment [DCE] authentication), including:

   1.1 management of approximately 40 high-level menu pages (these top-level pages would include site index maintenance pages), and

   1.2 preparation and management of approximately 50 pages of information updates from the unclassified Web site once a month.

   Web-content work to be covered consists of preparation of material (such as text, tables, forms, and related graphics) for Web presentation. The prepared material may include database-driven pages assembled by an existing Web application for presentation. This scope of work does not include development of new Web-based applications that process transactions or create or manage databases for persistent storage.

2. Management of Web Content Configuration: Maintain quality and currency of classified intranet and Internet content (information pages). Manage data associated with the information placement and maintenance procedure(s) for the classified Web environment.

3. Provide online computing information for classified users including some information (e.g., “getting started for classified users”) on the unclassified Web.

4. Management of Web information servers in the classified environment, providing the services described below. All information on the classified home page servers is unclassified. Includes accessibility mechanisms for NWC remote users authenticated via DCE:

   4.1 https service,

   4.2 user directory services (WebWHOS, etc.) for all employees, subcontractors, and NNSA/DOE, including classified e-mail address and secure telephone unit **(**STU) phone number when they exist,

   4.3 server-based Web application support tools (covered under 3.2.9 Classified Systems Administration),

   4.4 developer support for server-based tools plus commonly needed functional tools (e.g., inactivity timeout tools, DES encryption modules, account/work order validation routines), and periodic transfer of updated information (and applications, when needed) from unclassified environment to the classified Web information server. Assume updates twice a month.

5. Assist in migration of traditional Web site to content and applications, including collaboration, delivered via the SAP portal toolset. BWXT Y-12 is currently evaluating the SAP portal toolset and plans a phased implementation over the next 12–18 months.

Assist in the planning and implementation of the migration of the classified Web site to the new delivery mechanism. Answer questions, provide guidance, and develop Web information in support of information providers, Web users, and application developers.

3.2.2.2.4 Classified Software Product Update Delivery System

Provide a server-based network software delivery method for users connected to the classified network. This process should allow users who are licensed via the existing unclassified licensing infrastructure to access software installation folders located on the classified network.

3.2.2.2.5 Classified Desktop Office Visits

Provide office visits when needed to resolve desktop computing software problems for supported software.

3.2.2.2.6 Classified HelpDesk Service

Provide support for specified products and versions of software for desktop PC systems. Telephone assistance or alternative consulting support methods may be used to provide the most effective problem resolution. Hours of operation and other stipulations are covered under unclassified support specifications. (See 3.2.1.2.2 HelpDesk Service).

3.2.2.2.7 Classified Diskless Workstation Support

Provide initial configuration and support for approximately 400 users of diskless workstations (mostly “thin clients”), using the same set of supported software configured as in regular classified desktops. Support includes troubleshooting user problems and providing documentation describing: the requirements for migration; how to migrate to the new environment; and how to perform standard desktop services in the diskless environment.

3.2.2.2.8 Classified SecureNet User Support

Support SecureNet users in NWC cross-site functionality by:

1. using Secure Shell to provide secure file transfer protocol (FTP) service for communication between sites,

2. using X-emulation to run remote UNIX-hosted applications,

3. connecting to other sites’ resources via remote proxy machines, and

4. trouble-shooting and problem identification when users have difficulty with cross-site functions.

3.2.2.2.9 Virus Protection and Cleanup

1. Administrative/HelpDesk support for virus clean-up incidents on classified desktops, as directed by Computing Security and the IS&T organizations. Telephone assistance or alternative consulting support methods may be used to provide most effective problem resolution.

2. Office visits, when needed, for software virus cleanup (including resolution of virus attacks) as directed by the Computing and Telecommunications Security Organization (CTSO). This work shall consist of scanning and cleaning infected systems using CTSO-approved tools.

3.2.2.2.10 Public Key Infrastructure

1. Support for the classified Entrust Public Key Infrastructure (PKI) system console functions according to the NNSA Classified PKI Certificate Policy and Y-12's Classified Certification Practice Statement (CPS). This includes configuring Certificate Authority equipment and software, serving as Master Users or First Officers for certain formally defined procedures, and securely managing associated passwords and key tokens.

2. User registration and user support services (i.e. serve as Registration Authorities) for Classified Entrust PKI service, including adding new users into the Entrust directory, authenticating user identities face-to-face, assisting users with installation of Entrust desktop software and subsequent problems.

3.2.2.2.11 Classified Miscellaneous Support

Bi-monthly informal reporting on desktop service utilization to facilitate trend analysis and strategic planning of enterprise computing resources. This information may be combined with unclassified reporting and may be provided via e-mail or network database reports. Reported information shall include: number of classified user IDs; number of classified accounts; and number of e-mail accounts.

3.2.2.3 Performance Requirements

Response times shall be based on method of request, priority of request, and method of resolution required (see 3.2.1.3 Performance Requirements).

3.2.3 Unclassified Networking Services

3.2.3.1 Introduction

Unclassified network operation, administration, monitoring, management support, and design support services to unclassified network services are available 24 hours a day/7 days a week. This service includes the administration of the local area network (LAN) which is known as the Unclassified Services Network (USN).

Unclassified network support services include the administration, monitoring and technical support of the USN, and support of the approximately 300 network devices connected to the USN. These network devices include:

- routers,
- switches,
- Virtual Private Network (VPN) servers,
- Point-to-Point Protocol (PPP) servers,
- firewall,
- Domain Name Service (DNS) servers,
- Dynamic Host Configuration Protocol (DHCP) servers,

- network management servers,
- modems, and
- other to-be-determined network devices connected to the USN.

This service includes support for the approximately 6500 unclassified network LAN ports in use. Currently, these unclassified network LAN ports are divided between 10MBps and 100MBps switched Ethernet devices. Most central servers connected to the USN require gigabit interfaces.

The USN operates on a gigabit backbone connected with Cisco 6509 routers. Network hardware consists primarily of Cisco switches and Cisco routers. There are a limited number of other manufactures' switches still in operation; however, managed switches are being upgraded to Cisco switches throughout the site. Remote management and monitoring tools include CiscoWorks and HP OpenView.

Wide Area Network (WAN) connections include T1, Fractional T1, or high-speed digital subscriber line (HDSL) circuits. Remote access is offered through a PPP dial-up connection and over the Internet via VPN. WAN equipment in use includes LarseCom channel service units/data service units, ADL and PairGain HDSL synchronous data units and bridges, a Timeplex T1 multiplexer, a Racal Datacomm Omnimux 8000 Multiplexer, and various subrate modems and data service units.

The USN runs on fiber to most buildings on-site. Gigabit service is provided to building wiring closets with user connections from the building wiring closets to the desktops primarily over Cat 3 through Cat 6 unshielded twisted pair cabling. User requests for gigabit service to the desktop are handled on a case-by-case basis. Most central services requiring gigabit service are in the main computing facilities.

An intersite gigabit backbone connects the USN to the other sites on the Oak Ridge Reservation (ORR) including UT Battelle (Oak Ridge National Laboratory [ORNL]). Connectivity to the Internet for Y-12 National Security Complex is via the DOE Energy Sciences Network (Esnet) at ORNL. The connection to DOE-ORO is currently via a 100MBps fast Ethernet connection through ORNL. This allows connection to DOEnet. Each facility on the ORR, including Y-12, is separated from the other ORR sites by PIX firewalls.

As part of the Configuration Management Program, the USN has a tightly integrated process for managing access to the USN and assigning Internet Protocol (IP) addresses. The IP address management system integrates the data collected from desktop inventory, DHCP servers, and network device management tools to provide a highly automated, secure process for managing switch port VLAN assignments and IP addresses to desktop PCs. This system uses a combination of Y-12-provided DHCP, DNS, and network management tools, and other applications to support HelpDesk and inventory collection provided through this contract.

Approximately 125 buildings are supported on the Y-12 National Security Complex. The primary operational sites supported for this effort are resident on the same LAN, with cable plant intact. Some external local sites at Commerce Park and Union Valley are considered to be part of the USN. Users at other remote locations access the USN as specified by the CTM.

Portions of this work require coordination with BWXT Y-12 internal labor resources or other DOE Contractors due to the provisions of existing bargaining unit agreements,

memorandums of understanding, or DOE Contracts. For example, Qwest (or successor) is under contract with DOE to install cabling (both fiber and copper) between buildings for the Y-12 National Security Complex. The Facilities, Infrastructure and Services (FI&S) network group is responsible for on-site installation of networking equipment not covered under the Qwest (or successor) contract, such as switches, routers and the installation of twisted pair and fiber lines within certain buildings.

USN "Network Management and Operations" includes support for network devices, network services (residing on supporting servers), and supporting toolsets (residing on supporting servers) on the unclassified services network (USN), where:

- **Network Devices** include routers, switches, VPN servers, PPP servers, and USN perimeter firewall;
- **Network Services** include DNS and DHCP;
- **USN Supporting Toolsets** include, but are not limited to: CiscoWorks, HP OpenView, MRTG, and out-of-band access terminal server; and
- **USN Supporting Servers** include the servers listed in Section 3.2.3.2.4 under Item 2 Server Support hosting the network services and supporting toolsets. See 3.2.6 Unclassified Server Administration and 3.2.7 Unclassified Database Administration.

USN Network Management and Operations also includes support for network nodes on or accessing the USN. **Network Nodes** include clients and servers that require network support to access networks or to communicate with external network nodes. This includes configuration assistance for proper operation of the network nodes, remote access, consulting, HelpDesk, development, implementation of automated configuration tools, and field services.

Tivoli Inventory, Tivoli Enterprise Console, and Remedy (or equivalents) shall be Contractor supplied. This includes: the framework, licensing, configuration, administration, and operation of Tivoli, Tivoli Enterprise Console (TEC), and Remedy.

Exclusions from PWS

This service excludes costs of network hardware and software maintenance/licenses, hardware components, and facility charges. This service does not include the actual physical installation of hardware on the USN including such equipment as switches, routers, cabinets, firewalls, and twisted-pair and fiber lines. Installation of networking equipment and circuits is the responsibility of FI&S and Qwest (or successor).

3.2.3.2 Services

The Contractor shall provide:

3.2.3.2.1 Project Management

Project management includes planning, communication, and development of processes and procedures:

1. Planning

   Develop planning and strategy documents supporting individual upgrade and operational services for the USN. These documents include requirement definitions, functional system designs, configuration strategies, event processing logs, and workflow management documentation.

2. Coordination and Communications

   Coordinate ongoing operational services between developers, network support team, HelpDesk, management, and users, as required. Coordinate activities that are outside the scope of this service, such as configuration management, desktop support, and server support. Host special and recurring meetings to coordinate the activities of all parties involved, as required. Provide monthly services status reports to track progress and highlight important issues. Monthly reports shall be in mutually agreed format and delivered to the CTM via e-mail.

3. Process and Procedures

   Formalize and document processes and procedures for the routine activities of USN management. Provide copies to USN management, as requested. Review and update processes and procedures on an annual basis. Document processes using USN manager-approved formats. Processes and procedures to be documented include, but are not limited to:

   - Configuration and deployment of new switches,
   - Configuration and deployment of replacement switches in the event of a failure,
   - Administration of firewall access lists,
   - Management of shuns on the firewall,
   - Addition of new subnets and VLANS,
   - Addition of new VPN groups,
   - Activation of unused switch ports,
   - USN Operating Procedures, and
   - USN Policies and Plans.

3.2.3.2.2 Supporting Toolsets Development and Configuration

The Contractor shall support toolsets used in deployment, administration, and operation of the USN:

1. Device Management Tools

   Develop and configure BWXT Y-12 provided tools for the management of the routers and switches. These tools shall support image and configuration storage, transfers of these images and configurations to the devices, processes for change management, processes for configuration control, and inventory reporting capabilities.

2. Network Monitoring Tools

   Develop and configure BWXT Y-12 provided tools for network device monitoring. These tools shall provide network device availability and performance monitoring. These tools shall also provide trend analysis reporting. The Contractor shall integrate these tools with the centralized event correlation engine Tivoli Enterprise Console (TEC) or Contractor provided equivalent.

3. Event Correlation Rules

   Develop and administer event correlation rules for the escalation, correlation, and forwarding of events from network devices to the centralized HelpDesk management system utilizing the Tivoli framework, Tivoli Enterprise Console (TEC) or Contractor provided equivalent, and Remedy or Contractor provided equivalent.

4. Call Management and Workflow Processing

   Be responsible for the ongoing integration of call management and workflow processing for network related issues into a centralized HelpDesk management system utilizing Remedy or Contractor provided equivalent system.

5. IP Address Management Systems

   Administer an IP address management system that integrates the data collected from desktop inventory, DHCP servers, and supporting toolsets to provide a highly automated, secure solution for managing switch port VLAN assignments, IP address allocation, and DNS registration. This system may utilize a combination of BWXT Y-12 provided DHCP, DNS, and supporting toolsets, and [Contractor's] tools such as Tivoli and Remedy or Contractor provided equivalent systems. This service includes the ongoing collection and processing of the USN inventory data.

3.2.3.2.3 Network Administration and Operation

The Contractor shall support network and operations activities in the following areas:

1. Device Configuration

   Configure network devices for deployment on the USN and utilize the supporting toolsets to deploy and manage network devices.

2. Administration

Perform routine network device administration such as configuration changes, Operating System (OS) upgrades, OS patches, security patches, access list modifications, tuning, and user administration. Utilize supporting toolsets for these administration services on the new Cisco switches and routers. Develop, document, and implement new procedures describing the administration of the USN, as necessary. Coordinate with internal and external Contractors to prevent, correct, or detect network problems and/or outages, and to determine causes and solutions.

Coordinate installation of network hardware and software, and recommend upgrades for performance optimization to support BWXT Y-12 work load projections. Recommend network consolidations, extensions, upgrades, and shutdowns. Work with the USN Manager to coordinate activities on the USN such as planning installations, issuing orders to Qwest (or successor), FI&S, and other Contractors or vendors, directing work, tracking progress, and interfacing with customers.

Provide oversight of network hardware and software maintenance agreements necessary to support the operation of network equipment and software. This activity involves interaction with vendors, procurement, bargaining units, and finance personnel. Specific activities include, but are not limited to, network hardware and software inventory, funds management, procurement recommendations, upgrades, extensions, and compliance.

This scope includes the administration of the following USN components. Other networking devices may be added as part of network upgrades and configuration changes.

2.1. Firewall

Management of the firewall, including the PIX OS, the firewall access-list, and the firewall configuration. This includes management of firewall shuns, coordination with cyber security personnel, reporting to the Computer Incident Advisory Capability (CIAC) as required, recommending changes, and responding immediately to requested changes by BWXT Y-12 management or computer security personnel for issues concerning computer and network security.

2.2. VPN Server

Management of the VPN server configuration and OS

2.3. PPP Server

Management of the PPP server configuration and OS

2.4. DNS Server

Management of the DNS server configuration and OS

2.5. Routers and Switches

Management of the routers and switches

2.6. DHCP Server

Management of the DHCP server, and integration with the DHCP infrastructure as part of the IP Address Allocation system

3. Operation

Insure operation and availability of unclassified LAN systems (currently approximately 6500 LAN ports in use). Perform day-to-day operations of backups, log analyses, troubleshooting, inventory management, and system event response for the network devices.

Provide specifications for the acquisition of maintenance items for hardware, systems software, backup systems, and any other IT components supporting network devices. FI&S shall carry out maintenance, installations, or replacement of components as directed by the HelpDesk or the USN manager, or a specified alternate.

Outages due to maintenance or move/add/change activities shall be scheduled at least five (5) business days in advance, when possible. Activities shall be performed during off-hours, and shall be subject to Change Management processes, BWXT Y-12 approval, and FI&S considerations.

4. Configuration Management

Develop and maintain up-to-date baseline system configuration documentation for supported network devices, as enabled by the supporting toolsets. Utilize configuration control reports, as enabled by the supporting toolsets, to document differences between the current network device configuration and baseline configuration for Cisco switches. Utilize provided change management processes to document, request approval, and track the implementation of major configuration changes such as Cisco IOS operating system upgrades and patches for production network devices.

Maintain existing USN network drawings and diagrams, and provide new drawings for proposed and implemented network configurations.

5. Monitoring 24 hours a day/7 days a week

Provide staff for 24 x 7 for monitoring the operation of the network. Personnel on-site for computer operations shall be cross-trained to perform network monitoring in the event that a network failure prevents off-site monitoring. Utilize network monitoring tools, event correlation rules, call management, and workflow processing systems in the 24 x 7 monitoring.

Fault detection and resolution activities shall be communicated by telephone or pager to the USN manager, or alternate, and on-site network support staff. The speed and method of these communications shall depend on the severity level of the problem, as defined by BWXT Y-12 CTM, the criticality of the network device on which the problem

was encountered, and the time of day at which the problem was encountered. Repairs should minimize the impact on normal operations. Timing of repairs requiring physical access to the network device(s) shall be coordinated with FI&S for work defined in their contract.

6. IP Address Management

   Operate the current IP address management system, or equivalent, including maintenance of inventory data to support the requirements of this IP address management system, or equivalent.

7. Performance Reporting

   Provide and maintain performance trend analyses, and service level reporting through automated online tools. Allow the USN Manager and alternates to view the data via Web access. Provide monthly reports to the USN Manager for the purpose of tracking USN network availability, as well as other statistical data as may be defined by the USN Manager.

8. Capacity and Technology Planning

   Identify equipment and firmware for network devices on the USN that need to be upgraded, and recommend possible solutions to optimize network operation. Provide technical advice to the IS&T on network related matters during weekly USN status meetings.

   Support budget development for services, as requested, in accordance with schedules, formats, and procedures.

3.2.3.2.4 Integrated Services

The Contractor shall interface and coordinate with personnel providing services listed below to insure schedules and deliverables are met. Integrated Services addresses customer and support services that are an integral part of this service delivery.

Note: The following services are covered in other sections of this PWS:

1. Consolidated Service Desk

   The consolidated service desk Tier 1 (i.e. 574-4000) is provided under 3.2.1 Unclassified Desktop Support Services, and therefore is not included under this Service. The consolidated service desk Tier 1 shall provide HelpDesk support for network issues. The terms of the current contract shall govern the call handling procedures, call tracking, hours of operation, escalation procedures, applicable metrics, and project management structure. Emergency after hours calls for network issues shall be routed to the 24 x 7 monitoring staff.

2. Server Support

   Unclassified System Administration (3.2.6) and Unclassified Database Administration (3.2.7) for the supporting servers, as listed below:

- CiscoWorks server
- HP OpenView server
- Firewall Syslog / Trivial File Transfer Protocol (TFTP) server
- Domain Name Servers (5)
- Old HP OpenView server
- Network Monitoring servers (2)
- PPP Server Administration server
- Terminal Server

3. User Documentation

   Provide and maintain the following end-user network support documentation, delivered on a web server:

   - VPN client installation and configuration instructions,
   - DHCP migration instructions,
   - Firewall exception request instructions,
   - Tivoli exception request instructions,
   - IP registration instructions,
   - DNS registration instructions, and
   - Other user instructions as requested by the USN Manager.

4. Contractor Supplied Materials

   Tivoli Inventory, Tivoli Enterprise Console, and Remedy or equivalent(s) shall be Contractor supplied. This includes: the framework, servers, licensing, configuration, administration, and operation of Tivoli, Tivoli Enterprise Console (TEC), and Remedy.

3.2.3.3 Performance Requirements

1. Services provided by the Contractor shall be available, timely and meet quality expectations.

2. The USN shall have a 99.95% service availability during the period 7 a.m. – 6 p.m. Monday through Friday. Contractor shall have a 99.85% level of service 24 hours a day/7 days a week. USN availability shall be tracked with monthly reports on status provided to the USN Manager.

3.2.4 Classified Networking and Communications Security Services

3.2.4.1 Introduction

The Contractor shall provide 24 hours a day/7 days a week availability of all end-user elements of Classified Services Network (CSN). The Contractor shall also provide communications security (COMSEC) management and administration support services 24 hours a day/7 days a week.

Classified networking services to be provided include:

- The management and administrative support of the classified network (approximately 1000 users and 3100 total ports).

Note that the definition of a CSN user differs from that of a computer user. The CSN user is the employee who has registered for the key to the Terminal Connection Box (a key lock device to control physical access by the user to the network). There are several instances of a single CSN user holding multiple different keys (typically this is a foreman on the manufacturing facility which is also commonly called the "shop floor"). Some number of shop floor staff (computer users) then use the keys to access classified systems.

There are 20 buildings on the classified network. The classified LAN and unclassified LAN are completely separate networks. Some buildings shall contain both classified and unclassified networks. Security for classified machines is managed by a separate network and by encryption.

- SecureNet is a WAN that connects the classified LAN to classified LANs at other DOE sites throughout the country. The connections allowing SecureNet to communicate across the nation use NSA-approved Type 1 encryption devices.

- A Network Encryption System (NES) unit provides encryption at standard Ethernet bandwidth, a FASTLANE system provides the same at ATM OC3 bandwidth, and a TACLANE at 100 Mbps.

- A redundant Cisco PIX firewall provides perimeter protection for the CSN.The CSN includes "islands of security" located outside of the protected area. These are connected to the CSN via encryption devices called TACLANEs.

- Management and operations of the NES, FASTLANE, and TACLANE encryption devices, the classified networking equipment associated with these devices and a management station for the TACLANE devices are included in the scope of this Service.

COMSEC support services to be provided consist of the management and administrative support of the Communications Center. This includes the Secure Information Management Exchange System (SIMEX) and Automated Defense Information Network (AUTODIN) WAN network interfaces, the COMSEC officer duties for Y-12, and secure telephone unit (STU)-III/secure terminal equipment (STE) management (approximately 250 devices).

Note: STU delivery and tracking is performed by BWXT Y-12 to the other site contractors (UT Battelle and Becthel Jacobs [or successors]).

3.2.4.2 Services

3.2.4.2.1 Classified Network Support

The Contractor shall:

1. Insure the operation and availability of the CSN. Provide network administration and performance monitoring with 24 hours a day/7 days a week availability. Coordinate the installation and maintenance work performed by the FI&S organization.

   The Contractor shall accomplish this support by:

   1.1. Maintaining network engineering and technologist support on-site during normal operating hours (Monday–Friday, excluding holidays, from 7:30 a.m. until 5 p.m.) of

the CSN that covers the classified network of approximately 3100 ports, 1000 users, 125 switches, 4 hubs, 2 KGs, 1 Asynchronous Transfer Mode (ATM) switch, 1 NES, 2 FASTLANEs, 8 TACLANEs, 4 routers, and encompasses 20 buildings.

1.2. Providing user support available via HelpDesk 24 hours a day/7 days a week.

1.3. For hours outside the normal operating hours of the CSN, a call-in list of network support personnel is provided and on file with the CTM.

2. Provide development and communication of procedures applicable to the operations, maintenance, and security requirements of the CSN. Procedures shall adhere, as necessary, to the principles defined in the current version of the Conduct of Operations Manual (Y14-001).

3. Maintain operational statistics to include the following items: trunk availability and the number of authorized users, active ports, inactive ports, total ports, trouble calls, and information calls. Maintain operating statistics and equipment usage and availability information on Excel spreadsheets. Monthly operational statistics reports shall be issued 5 working days after the end of the calendar month. Maintain statistics and reports on Terminal Connection Boxes (TCBs).

4. Maintain a CSN equipment and port database that includes: equipment cabinet location, patch panel number, type of connection, network interface unit, device description or security plan number, lock key serial number, user division, faceplate number, and memorandum of understanding number.

5. Conduct, or assist with, required classified audits for NNSA Headquarters (NNSA-HQ). Assume that up to four (4) such audits shall be required annually.

6. Provide performance analysis and optimize resource utilization. Monitor workload and system performance information. Initiate routine upgrades of classified network hardware and software, and recommend upgrades for performance optimization to support BWXT Y-12 workload projections. Recommend network consolidations and shutdowns.

7. Provide oversight of classified network hardware and software maintenance agreements necessary to support the operations of network equipment and software. This activity involves interactions with BWXT Y-12 and vendor personnel. Specific activities include, but are not limited to, classified network hardware and software inventorying, funds management, procurement recommendations, upgrades, extensions, and compliance.

8. Provide configuration management for classified network systems software, hardware, and media.

9. Provide recommendations for infrastructure and process improvements, architectures and standards improvements, and new technologies that would reduce operational costs and/or significantly improve the level of service. These recommendations shall be provided informally via discussions among the Contractor's staff and the CTM.

10. Support the BWXT Y-12 budget development for activities noted in this service, on an annual basis, in accordance with BWXT Y-12 schedules, formats, and procedures. Estimates shall be derived from BWXT Y-12 requirements, anticipated workloads, and

funding levels. Responses to inquiries and questions shall be documented and completed in a timely manner.

11. Provide FASTLANE and TACLANE System Administrator functions to include:

    - Audit log monitoring and archival
    - Configuration functions
    - Key management

12. Provide documentation and procedures for routine Services required in the operation of the CSN, including:

    - Configuration of switches and routers
    - Configuration the firewall
    - Configuration of VLANs and subnets
    - Configuration of access lists
    - Configuration of encryptors.

13. Configure and manage provided tools for the management of routers and switches. These tools shall support image and configuration storage, transfers of these images and configurations to the devices, processes for change management, processes for configuration control, and inventory reporting capabilities. Configure and manage provided tools for network device monitoring. These tools shall provide device availability and performance monitoring.

14. Provide and manage configuration of network devices for deployment on the classified services network. Insure standardized configurations of similar network devices.

15. Perform routine network device administration, such as configuration changes, operating system (OS) upgrades, OS patches, security patches, access list modifications, tuning, and user administration for network devices.

16. Perform day-to-day operations of backups, log analyses, troubleshooting, device inventory management, and system event response for network devices.

17. Maintain existing non-engineering network diagrams and provide new drawings of all proposed and implemented configurations included under this award.

18. Provide specifications for the acquisition or maintenance for hardware, systems software, backup systems, and any other IT components supporting network devices.

19. Schedule outages due to maintenance or planned upgrades at least five business days in advance, if possible. Maintenance and upgrade activities shall be performed during off-hours and subject to CSN Manager approval and FI&S considerations.

20. Develop and maintain up-to-date baseline system configuration documentation for supported network devices. Fully document change requests and prepare required documentation for approval.

21. Communicate fault detection and resolution activities to the CSN Manager in a timely manner. The timing of these communications shall depend on the severity level of the problem, the criticality of the network device on which the problem was encountered,

and the time of day at which the problem was encountered. Repairs requiring physical access to the network device shall be coordinated with the FI&S organization. Scheduled repairs should be accomplished at such times as to minimize impact on the CSN, when possible.

22. Provide operational support for the redundant Cisco PIX firewall, including:

    - Administration of firewall rules (access lists)
    - Management of shuns on the firewall
    - Monitoring of firewall logs
    - Reports and statistics on firewall logs

23. Prepare and maintain the CSN Information System Security Plan (ISSP) and SecureNet Access Subnet (SNAS) IISP.

3.2.4.2.2 Communications Security Support

The Contractor shall:

1. Insure normal daily operation (7:30 a.m. to 5 p.m. Monday through Friday, excluding holidays) and 24 hours a day/7 days a week availability of the Communications Center. The Contractor shall provide Communications Center management and administration by providing COMSEC-certified computing technician support on-site during normal daily operating hours of the Communications Security Center. For all other times, a call-in list of COMSEC-certified support personnel shall be provided, posted at the facility and on file with the BWXT Y-12 Plant Shift Superintendent's Office. All COMSEC support personnel are currently NNSA COMSEC-trained and recertified every four (4) years. Upon completion of this training, these personnel may perform all functions (see DOE M 200.1-1 Telecommunications Security Manual) relating to NNSA COMSEC accounts.

2. Provide administrative support for acquisition, storage, assignment, distribution, inventory control, and accountability of COMSEC material. The Contractor shall provide administrative support for COMSEC material identified in the latest NNSA-HQ semiannual audit as follows:

    2.1. Assist in managing material controlled under a COMSEC Material Record System (CMRS) administered by NNSA-HQ.

    2.2. Assist NNSA-HQ by providing semiannual and annual audits of accountable materials for reconciliation.

    2.3. Assist in managing COMSEC material controlled and administered under guidelines specified in DOE M 200.1-1.

3. Provide the following SIMEX network support services:

    3.1. Planning – assist with SIMEX network security plan modifications and create local network plan attachments.

    3.2. Documentation – provide the CTM with SIMEX utilization statistics on a monthly basis and obtain CTM and Y-12 Site Office (YSO) approval of local security plans.

3.3. Implementation – COMSEC personnel shall have received both formal SIMEX training as well as on-the-job SIMEX training. Incoming and outgoing daily SIMEX traffic shall be administered by COMSEC certified computing technicians.

3.4. Monitoring – traffic utilization and log-in/log-off attempts to SIMEX node.

4. Provide development and communication of procedures and network support services for operation and maintenance of SIMEX and AUTODIN network interfaces. Procedures shall be prepared in accordance with the current version of the Conduct of Operations Manual (Y14-001).

   Note: The equipment is to be used only for official business and no software other than official SIMEX operating software shall exist on the local node system.

5. Provide quarterly reports of Communications Center activity to the CTM. This report shall consist of an Excel spreadsheet with the following fields: BWXT Y-12 department, charge number, and breakout of work by hours per month for the quarter. Quarterly Communications Center Activity reports shall be issued 10 working days after the end of the Government fiscal quarter.

6. Provide monthly statistical operational traffic reports on Communications Center activity to the CTM. This report shall consist of a billing report for the SIMEX terminal (narrative message) fields as follows: breakout of characters and messages received and transmitted via SIMEX by each message category. Monthly Statistical Operations Traffic reports on all Communications Center activities shall be issued 5 working days after the end of the calendar month.

7. Provide quarterly reports on secure telephone activity to the CTM. The STU/STE Database is provided as an Excel spreadsheet with the following headings: serial number, employee name, badge number, phone number, building, room, issue date, division name, division number, department, plant, and charge number. Quarterly Secure Telephone Activity reports shall be issued 5 working days after the close of the quarter.

8. Install STUs/STEs (approximately 250 STU devices), STU/STE data devices, and associated classified and encrypted equipment such as crypto-ignition keys (CIKs).

9. Provide training for STUs/STEs, STU/STE data devices, and associated classified and encrypted equipment such as CIKs. Provide administrative and clerical support for the acquisition of STEs and associated equipment.

   Contractor shall provide user training for individual STU/STE devices used within Y-12.

   Contractor shall provide support for the acquisition of STE devices and associated equipment (CIKs, power supplies, and batteries).

   Support shall include coordination by the COMSEC control officer with actual acquisition performed through the Service Manager and by BWXT Y-12 procurement elements.

10. Manage equipment inventories and provide quarterly activity reports for all STU/STE phones, STU/STE data devices, cryptographic keys, and keying material; and maintain

necessary spare equipment. Annual reports of cryptographic key and key material shall be provided to the NNSA Central Office of Record. The CIK database is provided as an Excel spreadsheet with the following column headings: number of units, CIK number, serial number, user, telephone number, building, room, issue date, and badge number. Equipment inventories are managed by the BWXT Y-12 COMSEC control officer through the BWXT Y-12 COMSEC custodians, administered by semiannual inventories provided by NNSA Central Office of Record, and locally generated using Excel spreadsheets.

11. Participate in classified audits for NNSA-HQ at ORR sites. Assume a formal NNSA-HQ audit shall be conducted once every two years and one annual formal on-site audit shall be conducted by the NNSA YSO at the local field office.

12. File required reports (SF153 COMSEC Material Report) with NNSA. The Contractor shall prepare and issue the SF153 reports, as required by NNSA.

13. Provide configuration management for COMSEC network and voice systems software, hardware, and media. Configuration management for COMSEC network and voice systems software, hardware, and media consists of the following:

    13.1. COMSEC equipment failures or modifications are coordinated with GSA or COMSEC approved vendors.

    13.2. NNSA approves all system hardware and software.

14. Provide recommendations for infrastructure and process improvements, architectures and standards improvements, and new technologies applicable to the PWS that would reduce operational costs and/or significantly improve level of service. These recommendations shall be provided informally via discussions among the Contractor's staff and the CTM.

15. Perform the duties of Building Emergency Warden position for two buildings. The Contractor shall provide services associated with the BWXT Y-12 Building Emergency Warden Plan.

16. Provide personnel to accommodate Criticality Accident Alarm System (CAAS) testing, as required.

17. Provide NES, FASTLANE, and TACLANE system administrator functions to include: audit log monitoring and archival, configuration functions, and key management.

3.2.4.3 Performance Requirements

1. Service provided by the Contractor shall be available, timely and meet quality expectations

2. The CSN shall have a 99.95% service availability during the period 7:30 a.m. – 5:00 p.m. Monday through Friday. Contractor shall have a 99.95% level of service 24 hours a day/7 days a week. CSN availability shall be tracked with monthly status reports provided to the CSN manager.

3. Service availability, response time, problem resolution, and overall service satisfaction regarding SIMEX and STU/STE operations shall be performed.

4. Turnaround time for problem resolution on the CSN shall be measured in accordance with the applicable CSN procedure. This procedure indicates that the turnaround time is dependent on the severity, impact, and time of occurrence of the problem. Different levels of turnaround time are described in the procedure.

3.2.5 Unclassified Computer Operations Services

3.2.5.1 Introduction

The Contractor shall provide 24 hours a day/7 days a week unclassified computer operations services including:

- monitoring and support of unclassified computer machine room operations and production systems;
- media library management;
- tape backups;
- vault storage of media;
- printed output management and distribution;
- development and maintenance of computer operations procedures;
- computing facility management; and
- job control.

Work shall be performed in accordance with DOE/NNSA orders and BWXT Y-12 procedures such as, but not limited to, those concerning Computer Security, Integrated Safety Management, Conduct of Operations, and Configuration Management.

This service includes total operations and management of the central unclassified computing environment. These centralized servers are physically located in three computing centers, within two buildings, inside the protected security area. The currently installed servers are listed in Appendix C-1 Section 1: Unclassified Computer Equipment. The computing environment changes on a regular basis, when new hardware and software are added, and older components are shutdown.

3.2.5.2 Services

The Contractor shall:

1. Provide support for the management and operations of unclassified computing resources and facilities. Support operation and availability of IT equipment, 24 hours a day/7 days a week, by providing the following services:

   - continuous monitoring;
   - backup;
   - input/output;
   - media management;
   - set-up and monitoring of applications, programs, production and distribution of printed and electronic output;

- outage recovery activities; and
- facility oversight of physical areas staffed by Contractor personnel.

2. Provide reduced operations support staff on weekends and the eleven (11) BWXT Y-12 holidays to the level required for computer room monitoring, disaster control, and minimal machine server operation.

   - On weekends, reduced support level shall be in effect from 4:30 p.m. on Friday until Monday at 8 a.m.
   - On BWXT Y-12's holidays, reduced support level shall be implemented for the 24-hour holiday period.

   The minimum staffing level at all times shall be two (2) employees.

3. Maintain a list of contacts for reporting system outages. Designated contacts shall be notified a minimum of two weeks in advance for any planned system outages of servers in Appendix C-1 Section 1: Unclassified Computer Equipment that include major system modifications or upgrades, such as: hardware configuration changes; operating system upgrades; or equipment movement.

   For planned system or service outages, the Contractor shall notify system users prior to the outage via e-mail (e.g., via a mailing list).

   If short-term planned outages occur due to system component failures or unexpected events, contacts shall be notified promptly as dictated by the situation.

   Contacts shall also be promptly notified in the event of unplanned system outages. For outages for which short-term notification shall be made, information provided shall include the cause of the outage, if known, and the expected service restoration time.

4. Maintain outage recovery procedures and contact lists for production servers monitored as part of this service. The content of these procedures may vary depending on Y-12's business needs and the importance of the server being monitored. These procedures may be as minimal as notifying the appropriate Contractor or BWXT Y-12contact employee responsible for effecting recovery services.

   Provide services to support recovery operations for servers that suffer outages or failures, including restoration from backup media, interaction with BWXT Y-12contacts regarding equipment replacement, and contact with equipment vendors regarding acquisition of services under existing hardware or software maintenance agreements.

   Recovery services shall include obtaining support, as required, from server administration and DBA personnel. Changes to outage recovery procedures shall be incorporated, as necessary, to adapt to the changing work environment.

5. Maintain information for those servers identified as "Applicable to Service Availability Metrics" in Appendix C-1, BWXT Y-12 Computer Equipment List, as necessary, for use in calculating Contractor performance metrics. Data collected shall include:

   - system name,
   - outage date, start time, end time, duration,

- name (and/or unique identifier) of contact employee most knowledgeable about the outage,
- text describing the service(s) affected [e.g., database management system (DBMS) operating system; application],
- outage cause(s), effects, resolution, notification time, and
- any other pertinent details.

The information shall include one of the following three qualifiers for each outage:

a. planned and approved by the CTM,

b. uncontrollable by Contractor, or

c. attributable to Contractor.

The information shall be made available electronically (e.g., via spreadsheet) to designated personnel, by the Contractor, as part of the metrics information for each designated metrics evaluation period. This information shall be included in the calculation of "Service Availability". Information collected by the Contractor related to server outages shall be used to calculate service downtime portion of the metric equation.

Availability metrics for certain end-user applications and systems applications on servers identified in Appendix C-1, Section 1 as "Applicable to Service Availability Metrics" shall be included in the calculation of "Problem Notification". The problem notification time, by Contractor staff, of problems affecting any end-user or systems application residing on servers designated in Appendix C-1, Section 1, Applicable to Service Availability Metrics, shall be included in this calculation, specifically for use in calculating "Average Notification Time." Outages that are planned and approved, or uncontrollable by the Contractor (e.g., power failures), shall not be used in the calculation of performance metrics.

6. Maintain a backup schedule for systems as approved by the CTM. Backup operations shall be performed consistently, in accordance with information contained in the approved schedule.

   Current backup frequencies are described in Appendix C-1 Section 1: Unclassified Computer Equipment. The backup schedule for any system shall be permanently changed only with the approval of the CTM.

   Transportation shall be provided for backup media to and from the site for satellite facilities, that require backup services.

   Support shall be provided for vault storage of media at a designated off-site location. Typical vault storage operations are performed each weekday.

   Recovery procedures may require accessing stored media from a remote vault. BWXT Y-12 shall provide the necessary vehicles for transport of media.

7. Maintain an accurate electronic inventory of stored media. Backup media shall be stored in a secure manner, obtainable on demand, by authorized personnel.

Media shall be removed from inventory only with the approval of the CTM, and shall be disposed of permanently only in accordance with BWXT Y-12 and NNSA-mandated requirements.

Media shall be available, on demand, for use in recovery operations.

On average, 40,000 unclassified media items are maintained in the Vertices Tape Management (Windows based) system, while legacy IBM unclassified tapes are maintained under the classified IBM CA-1 (tape management) and Control-M (scheduler). A full inventory of media is required on a quarterly basis.

8. Perform labeling, filing, retrieval, intra-building transport, and degaussing of media. Media shall be degaussed to support security requirements.

   Media shall be labeled properly to support inventory and security requirements.

   Media shall be pulled from filing locations per backup tape rotation requirements and re-filed after use.

9. Insure sufficient working stock levels of magnetic media as necessary to support the continuous operational cycle of scheduled system backup operations.

   Provide:

   - a one-month advance notification of the need to purchase magnetic media;
   - specification of media requirements;
   - actions necessary to obtain approvals from the CTM;
   - oversight of delivery and storage; and
   - other activities as necessary to maintain the required stock level of media to insure no impact on automated data processing operations due to shortages of media supply stocks.

10. Manage production and distribution of: reports; checks; check stubs; and electronic files. Files for printing and sealing the routine hourly, weekly, monthly, and retirement checks shall be made available by Contractor staff so checks and stubs can be printed.

11. Monitor working stock levels of media necessary to support continuous production of required output products. Provide one month advance notification of the need to purchase media, including paper, check stock, and other output media. Notification includes identifying media requirements, obtaining approvals from the CTM, and overseeing delivery and storage. Media stock levels ordered shall not exceed the capacity of available storage areas.

12. Provide prompt notification, with appropriate documentation, of errors/failures of production applications to appropriate identified contact(s).

13. Schedule periodic maintenance and related computer service commitments, as necessary to comply with warranty requirements and to insure on-going production operations, for each system, and provide local oversight of maintenance activities.

    Provide coordination of on-site vendor visits to the central computing-related facilities by BWXT Y-12 and/or vendor personnel for periodic maintenance, emergency repairs,

and other services. Coordination includes expediting access to equipment locations, escorting of non-cleared vendor personnel to computing-related facilities, and site preparation in advance of arrival of personnel (e.g., posting of security notices).

Outages required by service commitments shall be handled in a manner consistent with other planned outage-related requirements.

14. Insure proper marking, labeling, and handling of Automated Data Processing (ADP) related equipment, media and output as defined in Automated Information System (AIS) Security Handbook (Y19-401).

15. Conform to NNSA and BWXT Y-12 procedures, identified in Section J, Attachment E (List of Required Compliance Documents), regarding computer security. Regularly scheduled operations, or other activities described in this service, shall not be delayed by computer security failures on the part of the Contractor. Change operating procedures to adapt to changes in the operating environment.

16. Coordinate planning and execution of installation, modification, maintenance, and removal of equipment physically located in three computing centers, within two buildings, inside the protected security area. Obtain CTM approval for additions, modifications, or removals of ADP equipment within Y-12 National Security Complex.

17. Manage all levels of NNSA unclassified computing facilities and resources per DOE/NNSA orders and BWXT Y-12 computer security procedures and requirements, including preparation of computer security documentation.

    Maintain or provide input to documentation required by NNSA and BWXT Y-12 security guidelines, orders, and practices regarding operation of computer systems and network printers.

    Provide input, as requested, for plans and documents maintained by Y-12.

    Updates to computer security documentation maintained by the Contractor shall be prepared for BWXT Y-12 review and signoff one month prior to expiration of current documentation for a given server.

    Changes to procedures shall be incorporated as necessary to adapt to changes in the operating environment.

18. Provide Information Systems Security Officer (ISSO) deliverables and services required by NNSA/ BWXT Y-12 security procedures for Contractor-supervised systems and network printers. These systems shall include Contractor-operated desktop computer systems and certain server computers contained within Contractor-managed operations centers and offices.

19. Provide escorts for non-cleared visitors to Contractor operated classified computing-related facilities.

3.2.5.3 Performance Requirements

1. Services provided by the Contractor shall be available, timely and meet quality expectations.

2. The Contractor shall comply with service availability metrics, problem notification, and established resolution turnaround time.

3.2.6 Unclassified System Administration

3.2.6.1 Introduction

The Contractor shall provide 24 hours a day/7 days a week unclassified system administration support services. System administration includes support for products such as UNIX, Windows, OpenVMS layered systems products, including Exchange, Apache/IIS Web servers, systems management tools, and related peripheral equipment, such as printers (both network and directly attached) and tape drives. Specific system administration activities support a variety of unclassified applications, databases, e-mail, Web services, information management, file services, printing services, and computing infrastructure activities. Work shall be performed in accordance with DOE/NNSA orders and BWXT Y-12 procedures such as, but not limited to, those concerning Computer Security, Integrated Safety Management, Conduct of Operations, and Configuration Management.

Refer to 3.2.5.1 for current environment.

3.2.6.2 Services

The Contractor shall:

1. Provide 24 hours a day/7 days a week server and network printer administration, including:

- operating system installation, upgrades, and maintenance;
- system security-related sanitation;
- subsystem/layered system product support;
- backup and recovery services;
- system programming;
- configuration of peripherals; and
- consulting for problems/questions for servers listed in Appendix C-1, Section 1.

Administer firmware associated with network printers to provide special functions of network printing (i.e. user identification and printing).

Server computing systems shall be available for intended use 24 hours a day/7 days a week.

2. Insure appropriate Contractor or BWXT Y-12 contacts are notified promptly in the event of a server, server component, peripherals (i.e. network printers), or software component failure. Notification method and individual contacted shall be at the discretion of the Contractor for all servers, server and software components for which the CTM has not explicitly requested that BWXT Y-12 be contacted directly. Software components and products requiring contact notification include, but are not limited to: Oracle, Web Server software, Exchange mail server (including interface to external networks), print queues, SAP, UNIX, OpenVMS, Windows, and SQL-Server. Failure of such components and

products shall require support from the Contractor to accomplish recovery services.

3. Provide technical support for computer security policies, planning, documentation, access monitoring, and account/password distribution/revocation for servers and hosts.

   Server computers shall be secure in accordance with BWXT Y-12 and NNSA security procedures as defined in Section J, Attachment E (List of Required Compliance Documents).

   Server computer account and password mechanisms, systems, databases, and communications (to computer users, authorizers, CTSO, and other stakeholders) shall be up-to-date and in-sync, such that appropriate access is granted quickly and efficiently, but inappropriate access attempts and security-related occurrences are promptly detected and/or denied in a manner compliant with security policies.

   Prompt notification, with appropriate documentation, of any computer security occurrences shall be made to appropriate BWXT Y-12 representatives, including CTSO.

   Operating systems and layered products shall be up to date in accordance with computer security procedures and notifications from the CIAC.

4. Implement and administer configuration control procedures for hardware (including network printers), software, and network resources, and provide audit-reporting capability for Contractor-managed changes and modifications.

   The correct operational, installed version (per current systems configuration control documentation) of each major hardware and software component shall be present on each server.

   Examples of major components are processor manufacturer, type, and model; operating system; DBMS; major software components like Exchange, Web server software, Oracle, SAP, etc.

   Updated versions of these software components shall be tracked in the approved Configuration Management System (CMS).

   Configuration control documents and data, including change requests and associated data, shall be available to appropriate BWXT Y-12 personnel upon request.

   New procedures, or updates to existing procedures, shall be made for server configuration control, as necessary or desirable, to establish and maintain currency of configuration control procedures with the standards required by Y-12. Written approval by appropriate BWXT Y-12 personnel is required for such procedures/updates.

5. Maintain account concurrency among the majority of unclassified processors using UCAMS. Manage and distribute accounts and passwords via UCAMS, except in those cases where BWXT Y-12 business practices preclude this, or specify otherwise. When BWXT Y-12 business practices preclude the use of UCAMS, the Contractor shall provide a mechanism for the distribution of computer accounts and passwords which complies with stated security procedures.

6. Monitor server systems for resource utilization and system performance. Respond to inquiries regarding server performance. Insure server resources are configured such that performance and utilization are optimized.

7. Provide virus detection and removal for servers and hosts. Computer viruses and security-related occurrences (e.g., a classified e-mail message on an unclassified server) shall be promptly detected and resolved in a manner consistent with BWXT Y-12 security procedures, as defined in Section J, Attachment E (List of Required Compliance Documents). Prompt notification, with appropriate documentation, of any occurrences of the type listed above shall be made to appropriate BWXT Y-12 representatives, including CTSO.

8. Support preparation and issuance of purchase requisitions, orders, and contracts, and receipt and payment of invoices related to the initial purchase or renewal of computing-related products and services, including:

   - software licenses,
   - software/hardware maintenance agreements,
   - service agreements,
   - consulting agreements,
   - peripherals,
   - components,
   - commodities, and
   - other items that support IT activities.

   Maintain a list of technical and/or business contacts for each system, and/or component covered by server hardware and software maintenance contracts. Notification shall be provided to the appropriate contacts a minimum of 6 weeks before the existing contract's scheduled renewal date to insure that sufficient lead-time is available for contract renewals to occur.

   Provide guidance in selecting the appropriate technical configuration for software products prior to purchase.

   Invoice and payment information for existing contracts routed through BWXT Y-12 (i.e. HP, IBM, Oracle, etc.) shall be communicated to BWXT Y-12 CTM in a timely manner to insure prompt payment.

   Communicate with vendors to obtain quotes and resolve problems as part of the procurement cycle. Interface with Y-12's procurement, accounting, and other internal organizations to insure timely internal processing of procurement related materials.

   Enter procurement items electronically into SAP and assist with obtaining appropriate BWXT Y-12 approval for requisitions, orders, and invoices.

   Maintain an up-to-date spreadsheet of IT procurement items and associated data including:

   - item(s) procured,
   - model,
   - description,

- identification (node name, serial number, etc.) of the computer an item was bought for,
- vendor,
- detailed cost,
- expiration date,
- requisition/purchase order number,
- cost object, and
- technical contact name.

Note: The Contractor is not required to perform actual procurement activities such as legal issuance of contracts and issuance or payment of invoices.

9. Support administration and distribution of DBMS and other licenses purchased “in bulk” to internal Y-12 National Security Complex staff.

10. Provide programming support for the UCAMS application. This shall include programming support required to keep UCAMS applications operational due to software deficiencies, or unexpected UCAMS failures as a result of operating environment, system interface, or related problems. The Contractor shall provide installation of UCAMS central host and server (client side) software as program releases are made due to any modifications, including compilation of UCAMS software, under new operating or database management system versions. The Contractor shall provide appropriate software configuration management procedures, and documentation for the UCAMS application and its components.

11. Develop and maintain procedures related to server administration and network printer administration to support activities performed within the scope of this service

12. Support adjustments to the PWS described above for servers listed in Appendix C-1 and network printers. BWXT Y-12 requires regular adjustments to the list of servers and related software as listed. These adjustments shall include the addition and removal of computing components from the attached list. Examples include setting up operating systems and layered products on servers added to the list.

Server Additions and Deletions

1. Server additions typically fall into several categories:

    1.1. Acquisition of a new server and associated setup of the unit to perform as a file or print server, database server, and/or Web server.

    1.2. Replacement of an existing server with a new server to perform an identical function, typically to improve the hardware performance.

    1.3. Reuse of an existing server to perform a new function. For example, a database server may be reallocated as a Web server and no longer perform database functions.

    1.4. Setup of Network Attached Storage (NAS) device(s).

    1.5. Setup of a terminal server cluster, in a load-balancing configuration, to support a large group of desktop users. Servers in the cluster are essentially duplicates of

one another, and the cluster may be installed all at once or augmented over time.

2. The addition of a server shall include Contractor services necessary to prepare the server for a steady operational state, including:

   2.1. pre-purchase assistance regarding server procurements;

   2.2. installation and configuration of the base operating system, any compilers, and primary product or service configuration as described below;

   2.3. installation of scripts for monitoring, backups, and UCAMS;

   2.4. definition of directories and user profiles;

   2.5. providing input or preparing system security planning documents;

   2.6. configuration of network interface software, including security functions;

   2.7. facilitation and coordination of required equipment movement, installation, electrical work; and

   2.8. other services required to prepare server operation with BWXT Y-12 or vendor personnel.

3. Once the server is configured for operation, the Contractor shall provide ongoing operations, server administration, and database support services as described elsewhere within the PWS. BWXT Y-12 shall supply hardware and software required for a given server configuration. Prior to addition of a server to the server list, the CTM and Contractor shall agree on the necessary support levels shown in Appendix C-1.

   3.1. For file servers, setup activities shall include defining file shares and permissions and assigning users to groups.

   3.2. For print servers, setup activities shall include definition of network printers and print queues and assigning queues to printers.

   3.3. For Oracle DBMS servers, setup activities shall include installation of PL/SQL scripts for monitoring and backups; installation of the UCAMS client; creation of up to two databases and definition of table spaces and user profiles; installation of relational database management system (RDBMS) kernel and add-ons.

   3.4. For Web servers, setup activities shall include installation of Apache, Stronghold, or Netscape for UNIX; installation of IIS for Windows; installation of activity timeout handlers; installation of analog traffic analysis tools and CGI wrap; installation of SSL key.

   3.5. For Oracle Application Servers, setup activities shall include installation of PL/SQL cartridge package and procedures in the target database (up to three) and installation of forms and reports server.

   3.6. The deletion of a server shall require the Contractor to cease support for the server in question on a date specified by the CTM.

4. Table 6 identifies the base operating system, system configuration, and setup incremental adjustment variations that the Contractor shall support. Replacement

refers to the physical replacement of an existing server by another to perform an identical function. Reuse refers to reallocation of an existing server to perform a new function as shown.

Table 6. Items supported by the Contractor

Server type	Base operating system	Configuration	Adjustment types
Intel based	Windows NT, 2000, or 2003 Server	None	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	File server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Print server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Web server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Oracle DBMS server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Oracle application server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Base terminal server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Incremental terminal server in existing cluster	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	NAS server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Incremental NAS server in existing NAS cluster	Add, delete, replacement, reuse
Workstation	UNIX (Solaris, AIX, etc)	None	Add, delete, replacement, reuse
Workstation	UNIX (Solaris, AIX, etc)	Web server	Add, delete, replacement, reuse
Workstation	UNIX (Solaris, AIX, etc)	Oracle application server	Add, delete, replacement, reuse
Workstation	UNIX (Solaris, AIX, etc)	Oracle DBMS server	Add, delete, replacement, reuse
VAX/Alpha	OpenVMS	None	Add, delete, replacement, reuse

Note: For additional information concerning operating systems see Appendix C-1.

3.2.6.3 Performance Requirements

1. Services provided by the Contractor shall be available, timely and meet quality expectations.

2. The Contractor shall meet compliance requirements associated with resource utilization, system performance, security, virus protection, problem notification, and established resolution turnaround time.

3.2.7 Unclassified Database Administration

3.2.7.1 Introduction

The Contractor shall provide 24 hours a day/7 days a week unclassified database administration support services. Database administration includes support for products such as Oracle, Oracle Application Server, SQL-Server, SAS, and administration of commercial database software packages. Work shall be performed in accordance with DOE/NNSA orders and BWXT Y-12 procedures such as, but not limited to, those concerning Computer Security, Integrated Safety Management, Conduct of Operations, and Configuration Management.

Refer to 3.2.5.1 for current environment.

3.2.7.2 Services

The Contractor shall:

1. Provide production support to include operational coverage 24 hours a day/7 days a week, including event monitoring and alert notification for databases installed on servers listed in Appendix C-1, Section 1. Products to be supported include Oracle, Oracle Application Server, SQL-Server, and SAS.

2. Provide DBMS administration, implementation, and consulting support. Services provided include DBMS product installation, configuration additions, changes, and deletions.

3. Support DBMS configuration changes including, but not limited to, the following:

   3.1. user account and privilege maintenance,

   3.2. configuration of database system table spaces and indexes,

   3.3. sizing of database system table spaces and other storage areas based on BWXT Y-12 needs,

   3.4. security configuration,

   3.5. performance monitoring/tuning,

   3.6. debugging of DBMS performance and service problems,

   3.7. maintenance of utility services,

   3.8. maintenance of operating system/DBMS security interfaces, and

   3.9. other services required for support of DBMS setup and ongoing production and software development activities.

DBMS accounts, privileges, and passwords shall be maintained via UCAMS except in those cases where BWXT Y-12 business practices specify otherwise.

4. Perform DBMS implementation and related support activities in a manner which shall be consistent with NNSA and BWXT Y-12 security procedures. Changes to procedures shall be incorporated into the Contractor's normal daily operations as indicated by the CTM.

5. Provide responses to technical inquiries from the CTM regarding DBMS implementations, including configuration issues, DBMS error conditions and failures, security questions, backups, accounting, and system performance. Interface with DBMS vendors (such as Oracle), as required, in order to resolve technical support questions and other problems that cannot be resolved internally in a timely manner.

6. Maintain a list of installed DBMS tools and configurations (e.g., BWXT Y-12 designated server ID, product, version, etc.). Provide technical support for DBMS products, which shall be installed, configured, and maintained in accordance with applicable BWXT Y-12 standards and computer security guidelines, and as defined by the CTM and project requirements.

7. Support transfer of data into and between DBMS instances. The Contractor shall provide technical support for the movement of data among DBMS instances, including transfer of legacy data into upgraded DBMS instances. Routine database transfers of application data are excluded from this scope.

8. Provide support for DBMS configurations and procedures for backup operations and restoration of DBMS data and other system entities. This support includes:

   - providing for automated DBMS shutdown, backup, and restart cycles;
   - archive/redo log file sets;
   - rollback segments;
   - automated notification to appropriate personnel of backup cycle completion; and
   - other means of insuring database restoration upon demand.

   These configurations shall be implemented to perform within operating system parameters and software application requirements.

9. Maintain DBMS interfaces to server/host operating system platforms (e.g., UNIX, Windows, OpenVMS, etc.). Work with Server Administration and the CTM to define, specify, and maintain these interfaces. Perform DBMS implementation activities to insure consistency with operating system requirements, applications requirements, and other server operating environment requirements.

10. Provide installation assistance for upgrades and new versions of COTS software (e.g., Cyborg, Entrust, and Partnerworks) in accordance with CTM requests. Services associated with COTS-related installations including, but not limited to, migration of data in previously existing databases to the COTS package, integration of the appropriate version of the DBMS with the COTS package, configuration of the DBMS to work efficiently with the COTS package and associated software.

11. Develop and maintain DBA-related procedures to support the activities performed within the scope described herein.

12. Support adjustments to the PWS as described above for servers included in Appendix C-1, Section 1. BWXT Y-12 requires regular adjustments to the list of servers and related software.

3.2.7.3 Performance Requirements

1. Services provided by the Contractor shall be available, timely and meet quality expectations.

2. The Contractor shall meet compliance requirements associated with resource utilization, system performance, security, virus protection, problem notification, and established resolution turnaround time.

3.2.8 Classified Computer Operations Services

3.2.8.1 Introduction

The Contractor shall provide classified ADP operations support services 24 hours a day/7 days a week. Computer operations services required include monitoring and support of classified computer machine room operations and production systems, media library management, tape backups, vault storage of media, printed output management and distribution, development and maintenance of computer operations procedures, computing facility management, and job control. Work shall be performed in accordance with BWXT Y-12 procedures. Contractor employees are required to participate in the NNSA Human Reliability Program (HRP).

This service includes the total operations and management of the central classified computing environment. The current environment includes approximately 90 servers with hardware and software from a variety of vendors including, but not limited to, IBM, HP/Compaq, SUN, SGI/Cray, Microsoft, and Oracle. The currently installed servers are listed in Appendix C-1, Section 2. The computing environment changes on a regular basis when new hardware and software are added and the older components are shutdown. Servers are located on-site in two buildings containing three computing centers within the protected security area and are not accessible externally from public networks. Therefore, direct support of this service shall be performed at the Y-12 National Security Complex.

3.2.8.2 Services

The Contractor shall:

1. Provide management of classified computing facilities and resources per DOE/NNSA orders and CTSO directives and procedures, as defined in Section J, Attachment E (List of Required Compliance Documents.) The Contractor shall support computer operations and continuous availability of computer equipment and related services via activities including system monitoring, backup services, and outage recovery activities 24 hours a day/7 days a week. Details of computer operations support priorities and work activities shall be as defined below, and shall be negotiated and defined further by the Contractor and the CTM, as necessary, during the contract period to accommodate changes in the computing environment.

1.1. Operations support, on weekends and the 11 currently designated BWXT Y-12 holidays, shall be reduced to the level required to provide computer room monitoring, disaster control, and minimal machine server operation support. On weekends, the reduced operations support level shall be in effect from no earlier than Y-12's standard close of business on Friday evening (4:30 p.m.). Full support coverage by the Contractor shall resume on Monday morning no later than Y-12's standard start of business (8 a.m.). Every Sunday, additional staff shall be provided by the Contractor to service several of mission-essential applications. The time period for this support shall begin at 2 p.m. On BWXT Y-12 holidays, the reduced support level shall be implemented for the 24-hour holiday period. In order to comply with ISM requirements, the minimum staffing level for each operation's shift shall be two employees.

2. Maintain a list of BWXT Y-12 contacts, for reporting of planned system outages. Designated contacts shall be notified a minimum of two weeks in advance for any planned system outages that include major system modifications or upgrades, such as hardware configuration changes, operating system upgrades, or equipment movement. For planned system or service outages, the Contractor shall notify system users prior to the outage via e-mail (e.g., via a mailing list). If short term planned outages occur due to system component failures or similar unexpected needs, contacts shall also be notified promptly, as indicated by the situation. BWXT Y-12 contacts shall be promptly notified in the event of unplanned system outages. For outages requiring short term notification, the information provided shall include cause of the outage, if known, and expected service restoration time.

3. Maintain outage recovery procedures and contact lists for production servers monitored as part of Computer Operations. The content of these procedures may vary depending on business needs and the importance of the server being monitored. These procedures may be as minimal as notifying the appropriate Contractor or BWXT Y-12 contact employee responsible for providing recovery services. The Contractor shall provide services to support recovery operations for BWXT Y-12 servers that suffer outages or failures, including restoration from backup media, interaction with contacts regarding equipment replacement, and contact with equipment vendors regarding acquisition of services under existing hardware or software maintenance agreements. Recovery services shall include support as required from server administration and DBA personnel. Changes to outage recovery procedures shall be incorporated, as necessary, to adapt to the changing work environment.

4. Maintain information covering those servers specified as "Applicable to Service Availability Metrics" in Appendix C-1, Section 2, as necessary to provide Contractor performance metrics. This data shall include:

- system name,
- outage date, start time, end time, duration,
- name (and/or unique identifier) of contact employee most knowledgeable about the outage,
- text describing the service(s) affected (e.g., DBMS, operating system, or application), outage cause(s),
- effects, resolution, notification time, and
- any other pertinent details.

The information shall include one of the following three qualifiers for each outage:

- planned and approved by the CTM,
- uncontrollable by Contractor, or
- attributable to Contractor.

The information shall be made available electronically (e.g., via spreadsheet) to the CTM, by the Contractor, as part of the metrics information for each designated metrics evaluation period. This information shall be included in the calculation of the "Service Availability" portion of the metrics information. Information collected by the Contractor related to server outages shall be used to calculate the service downtime portion of the metric equation.

Certain end-user applications and systems applications on servers identified in Appendix C-1, Section 2, as "Applicable to Service Availability Metrics" shall be included in the calculation of the "Problem Notification" portion of the metrics information. The problem notification time, by Contractor staff, of problems affecting these systems, shall be included in this calculation, specifically for use in calculating "Average Notification Time." Outages that are planned and approved, or uncontrollable by the Contractor (e.g., power failures), shall not be used in the calculation of performance metrics.

5. Maintain a backup schedule for systems as approved by the CTM. Backup operations shall be performed consistently, in accordance with information contained in the schedule.

   Current backup frequencies are described in Appendix C-1, Section 1. The backup schedule for any system shall be changed permanently only with the approval of the CTM.

   Transportation shall be provided for backup media to and from the site for satellite facilities, that require backup services.

   Support for vault storage of media at a designated off-site location shall be provided. Typical vault storage operations are performed each weekday.

   Recovery procedures may require accessing stored media from a remote vault. BWXT Y-12 shall provide the necessary vehicles for transport of media.

6. Maintain an accurate electronic inventory of stored media. Backup media shall be stored in a secure manner, obtainable on demand, but only by authorized personnel. Media shall be removed from inventory only with the approval of the CTM, and shall be disposed of permanently only in accordance with BWXT Y-12 and NNSA-mandated requirements. Media shall be available, on demand, for use in recovery operations. On average, 12,000 classified media items are currently maintained in the tape library. A full inventory of media is required on a quarterly basis.

7. Perform labeling, filing, intra-building transport, and degaussing of media. Media shall be degaussed to support security requirements. Media shall be labeled in accordance with BWXT Y-12 and NNSA requirements, to support inventory and security requirements. Media shall be pulled from filing locations per backup tape rotation requirements and filed after use.

8. Insure sufficient working stock levels of magnetic media necessary to guarantee the continuous operational cycle of scheduled system backup operations. Contractor shall provide: a one-month advance notification of the need to purchase magnetic media; specification of media requirements; approvals from the CTM; oversight of delivery and storage; and other activities as necessary to maintain the required stock level of media to insure no impact on computer operations due to media supply stocks.

9. Manage production and distribution of production output, including reports and electronic files. The number of production application reports distributed include approximately 200 daily reports, 150 weekly reports, and 1000 reports that are monthly, quarterly, semiannual, annual, or on request. The approximate total monthly page count of printed reports is 110,000 pages.

10. Insure working stock levels of media (e.g., paper) required for production output sufficient to guarantee the continuous preparation of all output. Provide the CTM a 2-week advance notification of the need to purchase output media. This activity includes specification of media requirements, obtaining approvals from appropriate BWXT Y-12 personnel, oversight of delivery, and other activities necessary to maintain required stock level of output media.

11. Maintain a schedule, in support of Y-12's defined business needs, for selected processing and monitoring of production applications to insure schedules are met. A list of key contacts for reporting production output failures or delays shall be maintained. Provide prompt notification to designated contacts, with appropriate documentation, in the event of unplanned production output delays. Typically 10 calls per week are required. Production applications shall be consistently executed and/or monitored per the schedule and per Contractor and BWXT Y-12 procedures. Production application processing schedules shall be changed permanently only with the approval the CTM. On average, 50 production programs are initiated and 1100 are monitored for successful execution each week.

12. Schedule periodic maintenance and related computer hardware service for each system, and provide local oversight of maintenance activities. Provide coordination of on-site vendor visits to the central computer facilities by BWXT Y-12 and/or vendor personnel for periodic maintenance, emergency repairs, and other services. Coordination includes expediting access to equipment locations, escorting of non-cleared vendor personnel to computer facilities and site preparation in advance of arrival of personnel (e.g., posting of security notices). Outages required by service commitments shall be handled in a manner consistent with other planned outage-related requirements. The Contractor is not required to perform actual maintenance labor.

13. Insure proper marking, labeling, and handling of computer-related equipment, media and output in accordance with BWXT Y-12 requirements as defined in Automated Information System (AIS) Security Handbook (Y19-401INS).

14. Create and maintain a master list of accountable electronic removable media, to include a control number, date created/received, brief description, classification level and category, and disposition. The master list shall be a manual, paper-based, system and does not include barcode labeling or creation of an electronic database. Each removable media shall be labeled with the control number via a permanent marker or label. Labeling for up to 700 removable media is included in this service. An inventory

reconciliation of the master list shall be done up to four times a year.

15. Conform to BWXT Y-12 procedures regarding computer security. Regularly scheduled operations or other activities described in this service shall not be delayed by computer security failures on the part of the Contractor. Change operational procedures to adapt to changes in the operating environment.

16. Coordinate the planning and execution of the installation, modification, maintenance, and removal of computer equipment located in the central computing centers. CTM approval shall be obtained for additions, modifications, and removals related to computer equipment.

17. Manage all levels of classified computing facilities and resources per DOE/NNSA orders and CTSO procedures and requirements as amended, and provide input to computer security plans and other computer security documentation. Provide input to or maintain documentation required by BWXT Y-12 security guidelines, orders, and practices, to insure continuous operation of computer systems. The Contractor shall provide input, as requested by the CTM, to support system certification activities. Actual system operation shall be in accordance with BWXT Y-12 procedures and standards for classified computing equipment as specified in computer security documentation. Computer security documentation, maintained by the Contractor, shall be prepared for CTM review and approval two months in advance of the expiration of current documentation for a given server. Changes to procedures shall be incorporated, as necessary, by mutual agreement to adapt to changes in the operating environment.

18. Provide deliverables and services required by BWXT Y-12 security procedures of an Information System Security Officer (ISSO) for Contractor-supervised systems. This shall include Contractor-operated desktop computer systems and certain server computers contained within Contractor-managed operations centers and offices.

19. Provide escorts for non-cleared visitors to Contractor-operated computer facilities.

20. Insure site computer facility configurations are maintained to provide continuous operation of computer equipment. This includes location of equipment to insure maintenance access, efficient utilization of space to permit future expansion, oversight of heat loading versus HVAC capacity, and availability of power outlets and circuit boxes with electrical capacity necessary for safe operation. The Contractor shall perform the work in accordance with BWXT Y-12 procedures in conjunction with BWXT Y-12 computing equipment owners, vendors, and craft personnel.

    Note: The Contractor is not required to perform actual maintenance labor.

21. Maintain authorized personnel lists for central computer facilities as indicated by BWXT Y-12 guidelines for controlled access. Provide oversight of access to machine rooms in computer facilities, including review of the authorized personnel lists or issuance of local facility badge prior to permitting visitor entry, proper escorting of non-cleared visitors, visitor sign-ins, examination of parcels and briefcases for prohibited items, and other access requirements as mandated by BWXT Y-12 procedures. Support maintenance of cypher-locks, spin locks, and other local security devices related to computer facilities in accordance with BWXT Y-12 procedures.

Note: The Contractor is not required to perform actual maintenance labor.

22. Provide building management services for the two buildings that house Contractor-operated computing facilities, offices, and support facilities. The contractor maintains the only 24 hours a day/7 days a week presence in these buildings, and shall be responsible for support around-the-clock, including facility oversight during "off-shift" hours. Deliverables include prompt notification of contacts in the event of the failure of building support services including power, HVAC, lighting, elevators, and other services required to support continuous computer operations services provided by the Contractor. Create and maintain lists of BWXT Y-12 contacts for building support services for building management event notification. Coordinate routine maintenance and facility configuration change activities related to building support services, in accordance with BWXT Y-12 requirements in the areas of:

    - security,
    - fire,
    - safety,
    - health,
    - utilities,
    - operability,
    - building structural problems,
    - elevators,
    - mechanical rooms,
    - room keys,
    - janitorial service,
    - housekeeping,
    - vehicle usage, and
    - other building management services associated with computing facilities, offices, and support facilities operated and occupied by the Contractor as required to maintain the ongoing provision of continuous computer operations services.

    The Contractor is not required to perform off-shift walk-downs of the buildings, but shall contact appropriate BWXT Y-12 personnel in cases where abnormal occurrences are detected during these periods.

    Note: The Contractor is not required to perform actual maintenance labor.

23. Provide Building Emergency Warden services for two buildings that house Contractor-operated and occupied computing facilities, offices, and support facilities. Services include maintenance of facility emergency plans, updates to assembly point accountability rosters, coordination of periodic facility evacuation drills, and other supporting material required for compliance with Y-12 National Security Complex emergency preparedness. Services shall only apply to those personnel performing this PWS.

24. Provide environmental officer services for two buildings which house Contractor-operated and occupied computing facilities, offices, and support facilities. Services include facility environmental regulatory compliance communications, coordination, and training. Services shall only apply to those operations performed by the Contractor that require conformance to Y-12 National Security Complex environmental regulations.

25. Provide deliverables and services of a safety coordinator for two buildings, which house Contractor-operated and occupied computing facilities, offices, and support facilities. Services include issuance of safety work permits, coordination to ascertain that all safety requirements of lockout/tagout, the ISM program, and other BWXT Y-12 safety and reporting programs are followed with respect to Services involving applicable buildings. Services shall cover only those computing facilities, offices, and support facilities occupied by Contractor personnel and subcontractors employed by the Contractor, as required to maintain the ongoing provision of 24 hours a day/7 days a week computer operations services.

26. Provide deliverables and services required to support Conduct of Operations Manual (Y14-001) requirements for two buildings, which house Contractor-operated and occupied computing facilities, offices, and support facilities. Services include maintaining computer operations procedures describing the performance of activities within the scope of this service. Changes to computer operations procedures shall be incorporated, as necessary, by mutual agreement to adapt to changes in the operating environment.

3.2.8.3 Performance Requirements

1. Services provided by the Contractor shall be available, timely and meet quality expectations.

2. The Contractor shall comply with service availability metrics, problem notification standards, and establish resolution turnaround time.

3.2.9 Classified System Administration

3.2.9.1 Introduction

The Contractor shall provide classified system administration services 24 hours a day/7 days a week. Computer system administration includes support for products such as UNIX, Windows, OpenVMS, OS/390, layered systems products including Exchange, Apache/IIS Web servers, systems management tools, and related peripheral equipment such as printers and tape drives. Specific system administration activities support a variety of classified applications, databases, e-mail, Web services, information management, file services, printing services, and computing infrastructure activities. Contractor employees are required to participate in the NNSA HRP.

Refer to 3.2.8.1 for current environment.

3.2.9.2 Services

The Contractor shall:

1. Provide 24 hours a day/7 days a week server and host computer systems management and administration, including:

   - operating system installation, upgrades, and maintenance;
   - system security-related sanitation;
   - subsystem/layered system product support; backup and recovery services;
   - system programming;

- configuration of peripherals; and
- advice regarding problems/questions for servers listed in Appendix C-1 Section 2: Classified Computer Equipment.

Server computing systems shall be available 24 hours a day/7 days a week.

2. Insure that appropriate Contractor or BWXT Y-12 contacts are notified promptly in the event of a server, server component, or software component failure. The notification method and individual contacted shall be at the discretion of the Contractor for servers, server components, and software components for which the CTM has not explicitly requested that BWXT Y-12 be contacted directly. Software components and products included in this notification process, as used in this paragraph, may encompass systems-related applications including, but not limited to:

   - Oracle,
   - Web Server software,
   - Exchange mail server (including interface to external secure networks),
   - UNIX,
   - OpenVMS,
   - OS/390,
   - Windows,
   - SAP, and
   - CA-IDMS.

   Failure of such components and products shall require support from the Contractor to implement recovery services.

3. Provide technical support for BWXT Y-12 computer security policies, planning, documentation, access monitoring, and account/password distribution/revocation for servers and hosts.

   Server computers shall be secure in accordance with BWXT Y-12 and NNSA security procedures.

   Server computer account and password mechanisms, systems, databases, and communications (to computer users, authorizers, CTSO, and other stakeholders) shall be up-to-date and in sync such that appropriate access is granted quickly and efficiently, but inappropriate access attempts and security-related occurrences are promptly detected and/or denied in a manner compliant with security policies.

   Prompt notification, with appropriate documentation, of any computer security occurrences shall be made to the appropriate BWXT Y-12 representatives, including CTSO.

   Operating systems and layered products shall be up-to-date in accordance with computer security policies and/or notifications from the CIAC.

4. Implement and administer configuration control procedures for hardware, software, and network resources; provide audit-reporting capability for Contractor-managed changes and modifications.

The correct operational, installed version (per the current systems configuration control documentation) of each major hardware and software component shall be present on each server.

Examples of major components are:

- processor manufacturer, type, and model;
- operating system;
- DBMS; and
- major software components such as Exchange, Web server software, Oracle, etc.

Updated versions shall be as specified by appropriate configuration control instruments such as an approved Change Request. Configuration control documents shall be available to appropriate BWXT Y-12 personnel upon request.

New procedures or updates to existing procedures shall be generated for server configuration control as necessary to establish and maintain currency of configuration control procedures in accordance with the standards required by Y-12. Written approval by appropriate BWXT Y-12 personnel is required for such procedures/updates.

Configuration control activities shall be performed in accordance with the requirements of Appendix C Section 3.2.11 of the PWS.

5. Provide a process and mechanism to perform, in compliance with security procedures, management and distribution of computer access accounts and passwords for classified servers and Y-12-related NNSA SecureNet accounts. The mechanism currently used to maintain account concurrency among the majority of classified processors is UCAMS. The Contractor shall manage and distribute accounts and passwords via UCAMS except in those cases where BWXT Y-12 business practices specify otherwise.

6. Monitor server systems for resource utilization and system performance. Respond to BWXT Y-12 inquiries regarding server performance. Insure that server resources are configured such that performance and utilization is optimized.

7. Provide virus detection and removal for servers and hosts. Computer viruses and security-related occurrences shall be promptly detected and resolved in a manner consistent with BWXT Y-12 and NNSA security procedures. Prompt notification, with appropriate documentation, of occurrences of the type listed above shall be made to the CTM and the CTSO.

8. Support preparation and issuance of purchase requisitions, orders, and contracts, and receipt and payment of invoices related to obtainment/renewal of computing-related products. This includes software licenses, software/hardware maintenance agreements, service agreements, consulting, peripherals, components, commodities, and other items that support IT activities.

   Maintain a list of BWXT Y-12 technical and/or business contacts for each system and/or component covered by server hardware and software maintenance contracts. Notification shall be provided to appropriate BWXT Y-12 CTM a minimum of 6 weeks before the expiration of an existing contract to insure that sufficient lead-time is available for renewals to occur.

Provide guidance in selecting the appropriate technical configuration for software products, prior to purchase. Invoice and payment information for existing contracts routed through the Contractor shall be communicated to BWXT Y-12 CTM in a timely manner to insure prompt payment.

Communicate with vendors to obtain quotes and resolve issues and questions as part of the procurement cycle. Interface with Y-12's procurement, accounting, and other internal organizations to insure timely internal processing of procurement-related materials. Enter procurement items electronically into SAP and assist with obtaining appropriate BWXT Y-12 approval for requisitions, orders, and invoices.

Maintain an up-to-date spreadsheet of IT Procurement items and associated data, including:

- items procured,
- model,
- description,
- ID (node name, serial number, etc.) of the computer an item was bought for,
- vendor,
- detailed cost,
- expiration date,
- requisition/PO number,
- cost object, and
- technical contact name.

Note: The Contractor is not required to perform actual procurement activities, such as legal issuance of contracts and issuance or payment of invoices.

9. Support the administration and distribution of licenses for DBMS and other licenses purchased in bulk to internal BWXT Y-12 personnel.

10. Provide systems administration support to enable BWXT Y-12 participation in NWC SecureNet network connectivity with BWXT Y-12 partners at NNSA design laboratories (e.g., Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and Sandia National Laboratories) and production facilities (e.g., Pantex, Kansas City Plant, and Savannah River Site). SecureNet encompasses a classified network and related infrastructure to link NWC facilities across the United States. The activities performed shall include:

    - support for system administration functions related to operation of NNSA SecureNet and resources accessed via NNSA SecureNet;
    - server-level provisioning of DCE/DFS groups and accounts;
    - support for the exchange of files at the server level in a secure manner (e.g., SSH services); and
    - client functionality within the NNSA computing grid.

    NWC connectivity services provided by the Contractor shall include:

    - troubleshooting of server level connectivity issues,
    - server account management via UCAMS, and
    - systems support to enable Y-12's participation within NWC activities for servers defined in Appendix C-1, Section 2.

The Contractor shall support provisioning of local secure server access for BWXT Y-12 partners within the NWC who wish to access information resources located on servers defined in Appendix C-1, Section 2.

11. Provide programming support for the UCAMS application. This support shall include programming required to maintain the UCAMS applications operational status. This support shall include modifications related to BWXT Y-12 business rules and operating environment (e.g., operating system upgrade or DBMS changes).

    Provide installation of UCAMS central host and server (client side) software.

    Provide appropriate software configuration management procedures and documentation for the UCAMS application and its components.

12. Develop and maintain systems administration-related procedures to support the activities performed within the PWS.

13. Support adjustments to the PWS, as described above, for servers included in Appendix C-1 Section 2. BWXT Y-12 requires regular adjustments to the list of servers and related software. These adjustments shall include both the addition and removal of ADP components in Appendix C-1 Section 2.

    Server Additions and Deletions

    1. Server additions by BWXT Y-12 typically fall into several categories:

        1.1. Acquisition of a new server and associated setup of the unit to perform file or print server, database server, and/or Web server functions.

        1.2. Replacement of an existing server with a new server to perform an identical function, typically to improve hardware performance.

        1.3. Reuse of an existing server to perform a new function. For example, a database server may be reallocated as a Web server.

        1.4. Setup of Network Attached Storage (NAS) device(s).

        1.5. Setup of a terminal server cluster, in a load-balancing configuration, to support a large group of desktop users. Servers in the cluster are essentially duplicates of one another, and the cluster may be installed all at once or augmented over time.

        These categories are representative of server additions typically performed. Other types of additions shall be performed.

    2. The addition of a server shall include services necessary to prepare the server for a steady operational state, including:

        2.1. pre-purchase assistance regarding server procurements;

        2.2. installation and configuration of the base operating system, any compilers, and primary product or service configuration as described below;

        2.3. installation of scripts for monitoring, backups, and UCAMS;

2.4. definition of directories and user profiles;

2.5. providing input to or preparing system security planning documents;

2.6. configuration of network interface software, including security functions;

2.7. facilitation and coordination of required equipment movement, installation, electrical work, and other services required to prepare server operation with BWXT Y-12 or vendor personnel.

3. Once the server is configured for operation, the Contractor shall provide ongoing operations, system administration, and database support services as described elsewhere within the scope of this document. BWXT Y-12 shall purchase or supply all hardware and software required for a given server configuration. Prior to addition of a server to the server list, BWXT Y-12 and the Contractor shall agree on necessary support levels shown in Appendix C-1.

3.1. For file servers, setup activities shall include:

- defining file shares and permissions; and
- assigning users to groups.

3.2. For print servers, setup activities shall include:

- definition of network printers and print queues; and
- assigning queues to printers.

3.3. For Oracle DBMS servers, setup activities shall include:

- installation of PL/SQL scripts for monitoring and backups;
- installation of the UCAMS client;
- creation of up to two databases and definition of table spaces and user profiles; and
- installation of RDBMS kernel and add-ons.

3.4. For Web servers, setup activities shall include:

- installation of Apache, Stronghold, or Netscape for UNIX;
- installation of IIS for Windows;
- installation of activity timeout handlers;
- installation of analog traffic analysis tools and CGI wrap; and
- installation of SSL key.

3.5. For Oracle Application Servers, setup activities shall include:

- installation of PL/SQL cartridge package and procedures in the target database (up to three); and
- installation of forms and reports server.

4. The Contractor shall cease support for deleted servers on the date specified by the CTM.

5. Table 7 identifies the base operating system, system configuration, and setup incremental adjustment variations that the Contractor typically shall support. Replacement refers to physical replacement of an existing server by another, to

perform an identical function. Reuse refers to the reallocation of an existing server to perform a new function as shown.

Table 7. Items Supported by the Contractor

Server Type	Base Operating System	Configuration	Adjustment Types
Intel based	Windows NT, 2000, or 2003 Server	None	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	File server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Print server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Web server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Oracle DBMS server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Oracle application server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Base terminal server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Incremental terminal server in existing cluster	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Network attached storage (NAS) server	Add, delete, replacement, reuse
Intel based	Windows NT, 2000, or 2003 Server	Incremental NAS server in existing NAS cluster	Add, delete, replacement, reuse
Workstation	UNIX (Solaris, AIX, etc)	None	Add, delete, replacement, reuse
Workstation	UNIX (Solaris, AIX, etc)	Web server	Add, delete, replacement, reuse
Workstation	UNIX (Solaris, AIX, etc)	Oracle application server	Add, delete, replacement, reuse
Workstation	UNIX (Solaris, AIX, etc)	Oracle DBMS server	Add, delete, replacement, reuse
VAX/Alpha	OpenVMS	None	Add, delete, replacement, reuse

Note: See Appendix C-1 for additional information concerning operating systems.

3.2.9.3 Performance Requirements

1. Services provided by the Contractor shall be available, timely and meet quality expectations.

2. The Contractor shall meet or exceed resource utilization, system performance, security compliance, virus protection, problem notification, and established resolution turnaround time requirements.

3.2.10 Classified Database Administration

3.2.10.1 Introduction

The Contractor shall provide classified database administration services 24 hours a day/7 days a week. Database administration includes support for products such as Oracle, Oracle Application Server, CA-IDMS, SAS, and administration of commercial database software packages. Contractor employees are required to participate in the NNSA HRP.

Refer to 3.2.8.1 for current environment.

3.2.10.2 Services

The Contractor shall:

1. Provide production support to include 24 hours a day/7 days a week operational coverage, including event monitoring and alert notification for databases on servers listed in Appendix C-1, Section 2. Products to be supported include Oracle, Oracle Application Server, CA-IDMS, and SAS.

2. Provide DBMS administration, implementation, and consulting support. Services provided shall include DBMS product installation, configuration additions, changes, and deletions.

3. Support DBMS configuration changes, including, but not limited to, the following:

   3.1. user account and privilege maintenance,

   3.2. configuration of database system table spaces and indexes,

   3.3. sizing of database system tablespaces and other storage areas based on BWXT Y-12 needs,

   3.4. security configuration,

   3.5. performance monitoring/tuning,

   3.6. debugging of DBMS performance and service problems,

   3.7. maintenance of utility services,

   3.8. maintenance of operating system/DBMS security interfaces, and

   3.9. other services required for support of DBMS setup and ongoing production and software development activities.

   DBMS accounts, privileges and passwords shall be maintained via UCAMS except in those cases where BWXT Y-12 business practices specify otherwise.

4. Perform DBMS implementation and related support activities in a manner which shall be consistent with NNSA and BWXT Y-12 security procedures. Changes to procedures shall be incorporated into the Contractor's normal daily operations as indicated by Y-12.

5. Provide responses to technical inquiries from BWXT Y-12 regarding DBMS implementations, including:

   - configuration issues,
   - DBMS error conditions and failures,
   - security questions,
   - backups,
   - accounting, and
   - system performance.

   Interface with DBMS vendors (such as Oracle), as required, in order to resolve technical support questions and other problems that cannot be resolved internally in a timely manner.

6. Maintain a list of installed DBMS tools and configurations (e.g., Y-12-designated server ID, product, version, etc.). Provide technical support for DBMS products, which shall be installed, configured, and maintained in accordance with applicable BWXT Y-12 standards and computer security guidelines, and as defined by BWXT Y-12 and project requirements.

7. Support the transfer of data into and between DBMS instances. The Contractor shall provide technical support for the movement of data among DBMS instances, including the transfer of legacy data into upgraded DBMS instances. Routine database transfers of application data are excluded from this scope.

8. Provide support of DBMS configurations and procedures for backup operations and restoration of DBMS data and other system entities. This support includes:

   - providing for automated DBMS shutdown, backup, and restart cycles;
   - archive/redo log file sets;
   - rollback segments;
   - automated notification to appropriate personnel of backup cycle completion; and
   - other means of ensuring database restoration upon demand.

   These configurations shall be implemented to perform in concert with operating system parameters and software application requirements.

9. Maintain DBMS interfaces to server/host operating system platforms (e.g., UNIX, Windows, OpenVMS, etc.). Work with System Administration and BWXT Y-12 personnel to define, specify, and maintain these interfaces. Perform DBMS implementation activities to insure consistency with the configuration required by the operating system, BWXT Y-12 applications, and other server operational environment requirements.

10. Provide installation assistance for upgrades and new versions of COTS software (e.g., WorkStream from Applied Materials Corporation) per BWXT Y-12 request. Services associated with COTS-related installations including, but not limited to:

    - migration of data in previously existing BWXT Y-12 databases to the COTS package,

    - integration of the appropriate version of the DBMS with the COTS package, and

- configuration of the DBMS to work efficiently with the COTS package and associated software.

11. Develop and maintain DBA-related procedures to support the activities performed within the scope described herein.

12. Support adjustments to the PWS, as described above, for servers included in Appendix C-1, Section 2. BWXT Y-12 requires regular adjustments to the list of servers and related software.

3.2.10.3 Performance Requirements

1. Qualified personnel shall provide support services as outlined for classified database administration.

2. Services provided by the Contractor are available, timely and meet quality expectations.

3. The Contractor shall meet or exceed resource utilization, system performance, security, virus protection, problem notification, and established resolution turnaround time requirements.

3.2.11 Information Technology Configuration Management

3.2.11.1 Introduction

BWXT Y-12 manages its IT components via a procedure-based configuration management (CM) process. IT components connected to any BWXT Y-12 network are covered under the process. These components include servers, desktop computing hardware, network printers, network components (e.g., bridges, hubs, and routers), and Web areas.

A secondary aspect of this process is support for an inventory of specific IT components, to enable the overall effective management of the IT infrastructure. This inventory includes the ability to provide data to support audits, management decision-making, allocation of hardware and software, and related activities.

The Information Technology Configuration Management (IT-CM) process also supports enforcement of certain security and business policies by monitoring and reporting deviations. Finally, the process simplifies end user responsibilities in managing their computing devices in a secure manner.

Currently, several COTS tools are used to support IT-CM activities. The overall IT-CM process is automated to the greatest degree possible in the unclassified and classified environments, with the goal being to maximize automation and minimize the need for owners of IT components to interact with the system. Products currently in use include:

- IBM Tivoli in the unclassified environment for inventory acquisition, monitoring, and event processing for desktop devices and servers.
- BMC's Remedy HelpDesk software is used for trouble ticketing and change management processing for components in the unclassified environment. BMC's Remedy is also used for change management processing in the classified environment.
- HP Open View and Cisco Works are used for configuration management of network devices on the unclassified network, with Cisco Works in use on the classified network.

- Microsoft's Windows 2000/2003 Active Directory is in use in both environments for policy enforcement for Windows servers and desktops.
- Locally developed Web application software shall be used to interact with a back-end Oracle database used as a repository for the data generated by the IT-CM process.

Within Y-12's configuration management program, changes to components of the IT infrastructure are handled via a graded approval cycle. A common Web-based portal, currently using static pages, is utilized as a view into the IT inventory and CM system for network-attached IT components. This portal obtains its data from multiple sources, including a variety of COTS products that support the gathering of configuration data from the network-attached components.

Certain IT components have mandatory configurations, such as security settings, and deviations from these settings shall be flagged and reported promptly for remediation purposes. Exceptions to required configurations may be permitted under approved conditions, but shall be tracked. Automation of data capture related to IT components is an essential part of the IT-CM process.

The Contractor shall comply with the IT-CM process for classified and unclassified computing environments. Support of IT configuration management activities spans components used in other services described within the PWS. Configuration management work may be done by BWXT Y-12 as part of the individual services contained within this PWS.

Inclusions and Exclusions from Scope

For the unclassified environment, the Contractor shall supply services, including hardware and software, to support IT-CM activities, including IBM Tivoli and Remedy HelpDesk software or equivalent products, hosted on Contractor supplied servers. The Contractor shall also supply client (e.g., server, desktop) side Tivoli software or equivalent installed on Y-12's servers and desktops to support IT-CM activities. If equivalent software products are to be proposed, the Contractor shall define the process for migrating Y-12's current unclassified installation from IBM Tivoli and BMC Remedy in their proposal.

For the classified environment, BWXT Y-12 shall supply IT-CM related software and hardware. The Contractor shall supply on-site labor support only. Y-12-supplied software shall include Windows 2000/2003 Active Directory, Cisco Works, and BMC Remedy. BWXT Y-12 does not currently plan to use Tivoli in the classified environment.

BWXT Y-12 shall supply Windows 2000/2003, Active Directory, HP OpenView, and Cisco Works software and related hardware, for classified and unclassified environments. BWXT Y-12 shall supply servers to host the IT-CM portal and back-end database, along with required software licensing. These servers are listed in Appendix C-1.

The Contractor shall supply labor to maintain the IT-CM portal and the supporting database.

3.2.11.2 Services

The Contractor shall:

1. Provide IBM Tivoli and BMC Remedy software or equivalent products, hosted on Contractor-supplied servers, for the unclassified environment.

2. Provide IBM Tivoli or an equivalent solution for approximately 5500 network end points in the desktop and server environments and support inventory, and storage of inventory data for any of these devices connected to the BWXT Y-12 unclassified network at any time, for any period.

3. Provide BMC Remedy, or equivalent, to support work flow related to configuration management, and to implement graded change process management.

   The Contractor shall supply labor to maintain the hardware and software, perform upgrades and troubleshooting, and support BWXT Y-12 reporting needs using the data.

   On the server side, approximately two dozen changes per week are processed. On the desktop side, approximately 75 changes per week are processed. Desktop changes are not handled via formal change requests, but they are detected and logged using IBM Tivoli.

   Exceptions to desktop security or business configuration requirements are handled via the Remedy-based change management process.

4. Provide technical support for integration of HP Open View and Cisco Works data with the IT-CM portal and back-end Oracle database to support configuration management of unclassified network devices (e.g., bridges, hubs, and routers).

5. Provide support for configuration management of network printers for the unclassified environment. Currently network printers are handled as manual exceptions to the IT-CM process rather than via use of automated tools such as IBM Tivoli. These exceptions are processed using BMC Remedy change management software. There are approximately 250 network printers in use at Y-12; however, this number is expected to grow by 10% per year over the next 5 years.

6. Provide technical support for integration of data provided by IBM Tivoli and BMC Remedy (or equivalent) with the IT-CM back-end Oracle database and Web portal in accordance with BWXT Y-12 specifications.

7. Provide technical support for IT configuration management in the classified environment, using Y-12-supplied hardware and software. This support shall include technical support of BMC Remedy change management, and support of Cisco Works configuration management related activities. The support includes integration of data from these systems with the IT-CM back-end Oracle database and Web portal in accordance with BWXT Y-12 specifications.

8. Provide support for custom IT configuration management Web software and Oracle database maintenance in the unclassified and classified environments.

9. Provide support for Web-based reporting of IT-CM information in the unclassified and classified environments.

   Currently, information is obtained from the native data sources, such as IBM Tivoli, HP Open View, and Cisco Works, and reported via the Web, without intervening integration of data.

   BWXT Y-12 plans to roll out an integrated Oracle back-end database over the next two years to support robust Web-based reporting of data. BWXT Y-12 shall supply hardware and software to support these back-end reporting functions.

10. Support targeted auditing of IT components against a defined technical baseline, including audit reports, to ascertain compliance with security or technical policy in the unclassified and classified environments. This support shall be accomplished through the use of the IT-CM database and supporting tools such as IBM Tivoli (or equivalent), HP Open View, and Cisco Works.

11. Support changes to mandatory security and business configurations for the classified and unclassified environments. This shall include support for Windows 2000/2003 policy enforcement for Windows servers and desktops across Y-12. This work is included in 3.2.6 Unclassified Server Administration and 3.2.9 Classified Systems Administration.

3.2.11.3 Performance Requirements

Services provided by the Contractor shall be available, timely and meet quality expectations.

3.2.12 Applications Software Support

3.2.12.1 Introduction

The Contractor shall provide an application maintenance and enhancement environment in support of the business functions of Y-12.

Provide application development services in support of BWXT Y-12 business functions to include such activities as:

- planning support,
- project management,
- feasibility studies,
- requirements analysis,
- functional design,
- technical design,
- programming,
- package acquisition,
- testing,
- deployment,
- configuration management,
- maintenance, and
- retirement.

Manage designated applications and database assets to optimize Y-12's total investment in information technologies.

Enhancement services and maintenance and production support services are provided for applications that support the day-to-day business functions of Y-12. These applications consist of COTS packages, internally developed, and externally developed software. Specific applications are identified in Appendix C-2 BWXT Y-12 Applications.

3.2.12.2 Services

The Contractor shall:

1. Provide information software engineering services consisting of an application development environment having employees with the necessary experience, methods, tools, and technologies for planning, performing, testing, and deploying modifications to production applications and databases.

   Applications shall be developed or enhanced, tested, documented, and installed in accordance with BWXT Y-12 Management Requirements Y80-101PD, Software Management Program Description, and Y80-102INS, Software Management Instruction. Work shall be in compliance with BWXT Y-12 organization IT plans, strategies, and standard architectures and with applicable industry standards that support applications development and the use of COTS solutions.

2. Provide consultation and management services for project planning, scheduling, and oversight for large-scale IT initiatives.

3. Conduct assessments regarding feasibility and cost-benefit of COTS application packages, including large-scale enterprise resource planning systems, and develop appropriate implementation plans.

4. Develop requirement definitions, requirement analyses, cost-benefit analyses, and solution recommendations for automation of business processes using applications software.

5. Provide host, client-server, and Web-based application design and development services that include, but are not limited to, the following:

   5.1. Integration and implementation of COTS applications.

   5.2. Development in many software languages, including, but not limited to, C, C++, Java, JavaScript, HTML, SQL, PI/SQL, COBOL, SAS, CGI Programming, CICS, JCL, and VB.NET.

   5.3. Support of Windows NT, Windows 2000/2003, Macintosh, MVS, VMS, and various UNIX computing environments.

   5.4. Use of software engineering tools and integrated development environments, including, but not limited to, Visual C++, Visual Basic, Powerbuilder, Oracle Developer 2000 and Oracle Designer 2000, Microsoft Access and Excel, FoxPro, Cold Fusion, Microfocus Cobol, .net and ASP.

   5.5. Use of Oracle, DB2, CA-IDMS, Rdb, Ingres, and MS SQL Server DBMSs.

6. Provide application software production support, database management support for production data, production software configuration control, and disaster recovery to maintain application productivity.

7. Perform application software and database modifications necessitated by emergency situations and environmental changes to maintain production system availability.

   Perform other modifications as defined by the CTM.

   Applications software maintenance changes shall be performed, documented, tested, and installed in accordance with BWXT Y-12 management requirements, defined in 3.2.12.2.1 above. Specific applications shall require Y-12-approved authorization procedures and acceptance test plans. Such special requirements shall be defined by the CTM.

   Provide user consultation services for applications as requested by the technical contact(s), specified by the CTM.

8. Provide maintenance and annual testing of disaster recovery plans as required.

9. Provide application software asset inventories and information updates to Y-12's Software Application Manager (SAM) database.

10. Provide oversight of software maintenance agreements necessary to support and operate production applications. This activity involves interactions with vendor, procurement, and finance personnel. Specific activities may include software inventorying, reporting for funds control, upgrades, extensions, and compliance.

11. Support BWXT Y-12 budget development for these services on an annual basis, in accordance with BWXT Y-12 schedules, formats, and procedures. Estimates shall be derived from BWXT Y-12 requirements, anticipated workloads, and funding levels. Responses to BWXT Y-12 inquiries and questions shall be documented and completed in a timely manner.

3.2.12.3 Performance Requirements

1. Services provided by the Contractor shall be timely and meet quality expectations

2. Problem Notification/Resolution Turnaround Time – Turnaround time shall apply to applications support personnel and shall be measured from the time of discovery of an outage or time of notification by other support personnel across the Y-12 National Security Complex.

3.2.13 Enterprise Information Planning and Management

3.2.13.1 Introduction

Effective enterprise information planning and management are essential to achieving BWXT Y-12 mission objectives. There are two key components of BWXT Y-12 enterprise information management process. The first is an information strategy plan. This plan defines a desired future state condition, integrates IT initiatives across the enterprise in support of the future state, and provides a step-by-step roadmap for reaching the future state.

The second key component is a framework of IT architectures and standards. This architectural framework provides guidance covering the full range of information infrastructure requirements and issues, from strategic information systems planning through the final decommissioning and archival of legacy systems and data. The framework defines supporting processes, inventories, methodologies, and other necessary components of the enterprise information planning and management process.

Within Y-12, the CIO is responsible for planning and managing BWXT Y-12 enterprise information infrastructure. The service defined in this section supports the CIO, and others, as authorized by the CIO.

3.2.13.2 Services

The Contractor shall provide an innovative approach for supporting the CIO in planning and managing BWXT Y-12 information infrastructure. This approach shall address information resources used by BWXT Y-12.

The approach shall demonstrate how innovative IT practices shall be used to reduce costs, improve service, and enhance the overall competitive position of BWXT Y-12.

The approach shall also show how it shall leverage industry knowledge possessed by, or accessible to, BWXT Y-12 to achieve its objectives.

1. In support of BWXT Y-12 Defense Programs Strategic Plan, assist BWXT Y-12 in development of its semi-annual information strategy plan that defines a future state condition and a step-by-step roadmap for achieving future state objectives.

2. Assist the IS&T organization in provision of an enterprise information architecture and standards framework that best meets the needs of BWXT Y-12. Perform coordination and technology assessment activities necessary to keep this framework current. This framework shall include, as a minimum:

    2.1. A business model that characterizes business processes and their interactions,

    2.2. A technical architecture specification.

    2.3. An applications model reflecting as-is and future states.

    2.4. An information architecture that describes the information needs, databases, and information processes common to the entire enterprise.

    2.5. A hardware/network architecture with as-is and future-state views.

2.6. A roadmap of changes and services needed to reach future-state objectives.

3. Provide continuing support and expertise in the interpretation and use of BWXT Y-12 information architecture framework.

4. Provide support for supplemental as-needed enterprise information planning and management services. Examples of supplemental services include:

4.1. Facilitate the analysis, simplification, and reengineering of business processes

4.2. Perform special technology assessments and advise on adoption and assimilation of new technologies

4.3. Facilitate information systems planning sessions

4.4. Provide a reactive surge capability for critical events (assume 10 to 20 instances per year, ranging from one day to one month each)

4.5. Help organize requirements and metrics for IT service contracts obtained from multiple sources, creating a seamless, well-integrated IT support environment

4.6. Develop special plans and reports

4.7. Analyze and make recommendations on other enterprise information management problems or issues

3.2.13.3 Performance Requirements

Services provided by the Contractor shall be timely and meet quality expectations.

3.2.14 Special Computer Operations, System Administration, Database Administration, and Desktop Support

3.2.14.1 Introduction

The Contractor shall provide system and database administration, ADP operations support, and desktop support for various BWXT Y-12 divisions and projects. The services to be provided by the Contractor shall span projects across the business activities associated with BWXT Y-12 organizations, including:

- Engineering and Technology;
- Environment, Safety and Health;
- Occupational Health Services;
- Technology Development;
- Safeguards, Security, Counterintelligence, and Policy;
- Analytical Chemistry;
- Manufacturing;
- Human Resources; and
- other stand-alone projects.

Computer operations services required include:

- monitoring and support of Y-12 National Security Complex computer machine room operations and production systems,
- media library management,

- tape backups,
- vault storage of media,
- printed output management and distribution,
- development and maintenance of computer operations procedures,
- computing facility management, and
- job control.

Computer system administration includes support for products such as:

- UNIX,
- Windows,
- OpenVMS,
- OS/390,
- Stratus VOS,
- layered systems products including Exchange, Apache/IIS Web servers,
- system management tools, and
- related peripheral equipment such as printers and tape drives.

Specific system administration activities support a variety of classified applications, databases, e-mail, Web services, information management, file services, printing services, and computing infrastructure activities.

Database administration includes support for products such as Oracle and administration of commercial database software packages. Desktop support activities include support of office visits, consulting, and related activities.

Other support included in this service covers technical assistance for IT Services, document preparation, and requirements analysis.

The current environment includes approximately 250 servers, with hardware and software from a variety of vendors including, but not limited to, IBM, HP/Compaq, Sun, SGI/Cray, Microsoft, Stratus, Oracle, and others. The currently installed servers are as listed in Appendix C-1, Section 3: Other Computer Equipment.

The computing environment changes on a regular basis, with the addition of new hardware and software and the shutdown of older components. Servers are located on-site and some are not accessible externally from public networks. Direct support of this requirement shall be performed at the Y-12 National Security Complex. The servers are physically located in three main computing centers and other locations throughout the Complex.

3.2.14.2 Services

Note that support within this service may include information technology activities other than those listed specifically below.

Refer to Appendix C-1, Section 3 for computer operation support, system management support, and database management support levels.

3.2.14.2.1 User Services and Desktop Support

The Contractor shall:

1. Provide support for software and activities not covered in 3.2.1 Unclassified Desktop Support Services and 3.2.2 Classified Desktop Support Services.
2. Support security incident cleanup for user desktop personal computers and workstations.
3. Prepare and support Web pages and Web applications not covered in 3.2.1 Unclassified Desktop Support Services and 3.2.2 Classified Desktop Support Services.
4. Implement network utility functions and services to enhance the distributed computing environment, such as phone-server or DCE/DFS authentication functionality.

3.2.14.2.2 ADP Operations Services

The Contractor shall:

1. Manage and oversee computing service centers.
2. Provide data and document entry support.
3. Provide support for activities not covered in the 3.2.5 Unclassified Computer Operations Services and 3.2.8 Classified Computer Operations Services.

3.2.14.2.3 Systems Administration

The Contractor shall:

1. Assist in the preparation of reports and documents covering topics including capacity management planning, disaster recovery/contingency planning, performance planning, cyber security, and risk assessments.
2. Support computer security activities, including planning, documentation, and monitoring for servers, hosts, and desktops.
3. Support virus and security incident detection for servers, hosts, and desktops.
4. Evaluate and test COTS applications software at the direction of the CTM.
5. Provide system programming services for UNIX, Windows, OS/390, VOS, OpenVMS, and other platforms.
6. Support automated management and distribution of computer accounts and passwords. This shall include those activities required for software maintenance of UCAMS.
7. Support virus and security incident removal and/or system cleanup for servers, hosts, and desktops.
8. Install packaged COTS applications software on BWXT Y-12 servers and desktops.

3.2.14.2.4 Database Administration

The Contractor shall assist BWXT Y-12 to:

1. Prepare reports detailing written recommendations for DBMS strategies, upgrades, changes, consolidations, additions, and/or shutdowns that would optimize performance or otherwise improve DBMS operations and administration.

2. Provide recommendations regarding procurement actions and strategies that shall result in the lowest overall cost for DBMS products and support to Y-12.

3. Supply information regarding DBMS resource utilization, sizing, and performance statistics, reports and graphs for DBMS instances.

4. Prepare DBMS strategic management study and risk assessment reports.

5. Provide written recommendations to BWXT Y-12 regarding DBMS performance and capacity issues.

3.2.14.3 Performance Requirements

1. Services provided by the Contractor shall be timely and meet quality expectations.

2. See sections 3.2.1.3, 3.2.2.3, 3.2.5.3, 3.2.6.3, 3.2.7.3, 3.2.8.3, 3.2.9.3, and 3.2.10.3 for additional performance requirements.

3.2.15 Voice Communications Services

3.2.15.1 Introduction

The Contractor shall provide telephone, paging, cellular service, radio, and general voice and wireless management, operation, administration, and design support services to the Y-12 National Security Complex 24 hours a day/7 days a week.

Voice Communications support services to be provided include the management, operation, and technical support of site paging, cellular, FTS2000 voice systems, and conventional and trunking radio systems. Presently BWXT Y-12 has on-site approximately:

1. 2000 alphanumeric pagers,

2. 500 numeric pagers,

3. 200 in-plant pagers,

4. 200 cellular phones with 25 vehicle-mounted cellular units

5. 1600 hand-held portable conventional and trunked radios, and

6. 6400 telephone lines as part of the Oak Ridge Federal Integrated Communications Network (ORFICN).

ORFICN: The ORFICN is the official telephone system for the ORR, including the Y-12 National Security Complex. The DOE ORO office maintains the contract for the management and administration of the ORFICN with Qwest (or successor). BWXT Y-12 is charged a portion of the ORFICN contract cost annually by ORO. The contract expires in 2007.

PAGERS: In order to maintain a high level of paging coverage across the various sites and within campus facilities, a number of site-specific transmitting equipment is in place.

Voice Service engineering and support personnel work in conjunction with the BWXT Y-12 Plant Shift Superintendent (PSS) organizations to assure that this equipment is operational, and in cases where local coverage has been lost, work with vendor technical personnel to restore service.

Voice Service engineering and support personnel also provide equivalent backup and recovery support services for the in-plant local area paging system in the Y-12 National Security Complex.

Voice Services personnel also maintain a number of spare paging and cellular devices for use by BWXT Y-12 if their assigned device fails, or some special circumstance defines a need requiring a number of units for short-term usage.

Voice Services personnel conduct test pages to monitor the capabilities and response time of the wide area paging system on a regular basis. This system is increasingly used by the various site populations to not only send routine message and notification traffic, but to send traffic in support of critical site organizations (i.e., BWXT Y-12 PSS, Safety and Health, Protective Services, etc.) as well as provide automatic notification of specific system or process functions. Delays or degradation of messaging capabilities can adversely affect operations and the safety and health of the various operations across each site.

RADIOS: The current radio trunking system infrastructure at Y-12 National Security Complex includes encrypted and clear capability, T-1, and copper line connectivity (leased and owned) for remote trunking capabilities as well as connectivity with BWXT Y-12 conventional networks. Oak Ridge public safety organizations, 1 Motorola Smartnet II trunking central controller, 7 repeaters, 1 central electronics bank, 10 CRT dispatch consoles, about 40 desktop radios, 1 system management terminal, Smartnet Information Processors, and SystemWatch List are also included.

The Ultra High Frequency (UHF) radio trunking system at the Y-12 National Security Complex includes more than 1500 resident subscriber units and more than 70 non-resident subscriber units (ETTP and ORNL). A subscriber unit is either a portable hand-held radio or a mobile radio installed in a vehicle. Currently, the majority (almost 1,200) of BWXT Y-12's subscriber units are Motorola wideband, analog portable Systems Saber radios. Almost 200 BWXT Y-12 subscriber units are Motorola narrowband/wideband, analog portable MTS2000 radios. The current UHF system shall transition to a narrowband trunking system by January 1, 2008. All wideband radios shall have to be replaced by narrowband radios by that time.

The conventional radio system infrastructure at the Y-12 National Security Complex includes encrypted and clear capability, leased 4-wire for connectivity with the radio trunking system at the Y-12 National Security Complex, 12 repeaters and 1 desktop radio. The conventional radio system has more than 200 portable radios with about half Motorola and half General Electric models.

CELLULAR PHONES: Cellular phones are limited in use to certain areas of the Y-12 National Security Complex. Approximately 200 cellular telephones are in use. Cellular telephones with special features and personally owned cellular telephones are not allowed.

OTHER WIRELESS DEVICES: Wireless devices at the Y-12 National Security Complex shall be pre-approved by BWXT Y-12 management on a case-by-case basis. General purpose wireless devices such as Personal Data Assistants (PDAs) are not permitted. Wireless devices for special purposes are approved through a Telecommunications Proposal process.

Exclusions from Scope

This service excludes costs of network hardware and software maintenance/licenses; actual charges by paging and cellular Contractors to BWXT Y-12 and NNSA; hardware components; facility charges; and any scope/service of voice services currently provided by Qwest (or successor) Communications.

3.2.15.2 Services

3.2.15.2.1 Site-Only Telephone Support

The Contractor shall:

1. Provide administrative and technical support to users on the ORFICN at the Y-12 National Security Complex in planning for additions, deletions, and changes to their telephone services. This includes assisting organizations with moves and other changes involving their phone service, making recommendations, and handling problems.

2. Provide technical support of site telephone-related functions such as voice interfaces for the Tennessee Emergency Management Agency (TEMA), Emergency Preparedness, Plant Safety and Security, and the BWXT Y-12 PSS and E911 Systems (approximately 200 hours/month).

3. Analyze telephone service charges to insure proper billing to Y-12. Advise BWXT Y-12 Network Manager of any problems with billing.

4. Interface with ORO and Qwest (or successor) to provide corporate data necessary for site directory and 911 directory information. Insure information provided is consistent with BWXT Y-12 policy on information release. Update functional directory information annually.

5. Work with BWXT Y-12 organization telephone service coordinators to insure that they review their organization's telephone, cellular, and paging charges to verify that they are correct, analyze monthly bills posted on the Web, and make corrections.

6. Review the corporate Web pages for telecommunications services to insure information is current and making recommendations to BWXT Y-12 Network Manager on ways to improve information delivery to users.

7. Provide reports and other special information requests to the BWXT Y-12 CTM, as requested.

3.2.15.2.2 Cellular Telephone Support

The Contractor shall:

1. Provide cellular telephone system management and administration (approximately 200 hand-held and 25 vehicle-mounted cellular telephones).

2. Perform administrative system support, providing the interface between BWXT Y-12 and the cellular vendor on a daily basis. This effort involves installing new cellular accounts; closing, modifying, or upgrading existing cellular accounts; ordering and arranging for delivery/ installation of equipment; and providing backup and recovery services, development and communication of procedures, system monitoring, and technical assistance for problems/questions.

3. Maintain tracking information for each cellular telephone, such as add, delete, or change, etc., in an official inventory database with a Web interface. Database shall be maintained on a corporate IT server with regular backups. Provide a monthly status report of cellular telephone inventory to BWXT Y-12 Network Manager.

4. Maintain a copy of vendor(s) billing information and interpret billing costs as requested by Y-12; if billing data are not available, arrange to get a copy for BWXT Y-12 from the vendor.

5. Support the cellular award(s) between BWXT Y-12 and the cellular telephone service suppliers and develop technical specifications if requested for the base contract. Participate in the bid process with BWXT Y-12 procurement as technical advisors. Provide a technical evaluation of vendor claims, as it relates to coverage and recoverability. Coordinate contract extensions and modifications with procurement.

6. Assist the cellular telephone service supplier(s) technical personnel to resolve technical problems. Work with the vendor(s) to improve coverage conditions in concert with user requirements (e.g., establishing improved coverage between Oak Ridge sites, improving in-plant and area coverage, etc.).

7. Insure users of cellular telephones in the Y-12 National Security Complex understand the policies concerning wireless communications.

8. Insure processes involved in the administrative of cellular services at the Y-12 National Security Complex comply with established network, computer security, and NNSA policies.

3.2.15.2.3 Pager Support

The Contractor shall:

1. Provide paging system management and administration (approximately 2000 alphanumeric and 500 numeric pagers).

2. Perform administrative system support, providing the interface between BWXT Y-12 and the paging vendor on a daily basis. This effort involves installing new pager accounts; closing, modifying, or upgrading existing pager accounts; supporting the Web interface; ordering and arranging for delivery of equipment; programming group paging networks; and providing backup and recovery services, development and communication of procedures, system monitoring, battery provisioning, coordination of billing, and technical assistance to resolve problems/questions.

3. Maintain tracking information for each add, delete, change, etc., in an official inventory database with a Web interface. Database shall be maintained on a corporate IT server with regular backups. Provide a monthly status report of paging inventory to BWXT Y-12 Network Manager.

4. Support paging award(s) between BWXT Y-12 procurement and the paging service suppliers, and develop technical specifications for the base contract. Participate in the bid process with BWXT Y-12 procurement as technical advisors. Provide a technical evaluation of paging service suppliers as requested. Coordinate contract extension, modification, etc.

5. Coordinate with paging service supplier(s) technical personnel to resolve operational problems associated with antenna sites, transmitters, telephone interfacing, and automated paging interfaces between the DOE Oak Ridge Reservation system and the vendor. Work with the paging service supplier(s) to improve coverage conditions in concert with user requirements (e.g., establishing improved coverage and availability for nationwide paging; establishing improved in-plant and area coverage by adding antennas, etc.).

3.2.15.2.4 Radio Support

The Contractor shall:

1. Support conventional and trunked radios at the Y-12 National Security Complex (approximately 250 conventional radios and 1600 trunked radios on-site). Manage frequencies for the Y-12 National Security Complex; insure proper licensing, electromagnetic compatibility, spectrum interference, and inter-modulation are addressed; provide configuration control; develop and communicate procedures; and analyze requirements.

2. Manage the Y-12 National Security Complex trunked radio system. Manage and coordinate the various user trunk groups.

3. Provide technical and engineering expertise in the management, engineering, configuration, and regulation of the Y-12 National Security Complex radio system and equipment.

4. Maintain a corresponding database of radios for BWXT Y-12 with a Web interface. Database shall be maintained on a corporate IT server with regular backups. Provide a trunk group quarterly report for the reservation and for BWXT Y-12 Radio Manager.

5. Track monthly radio usage. Provide monthly radio reports to BWXT Y-12 Unclassified Network Manager and BWXT Y-12 Radio Manager.

6. Provide reports to BWXT Y-12 Radio Manager or BWXT Y-12 Unclassified Network Manager, on request, concerning various components of the Y-12 National Security Complex Radio Network.

7. Assist the BWXT Y-12 Radio Manager with the annual recertification and recall program for the Y-12 National Security Complex radio network, as requested.

8. Coordinate and manage annual radio communications inventory for DOE.

9. Coordinate and manage the Y-12 National Security Complex repeater site inspections for DOE.

10. Provide preparation of telecommunication proposals in accordance with National Telecommunication and Information Administration (NTIA) Chapter 9: FMS submissions to NTIA through DOE.

11. Provide frequency interference resolution support across the reservation.

12. Technically coordinate the leased sitting of commercial wireless providers per DOE and Government Services Administration directives, if requested.

13. Provide technical support and frequency coordination with local public safety entities for mutual aid requirements for BWXT Y-12.

14. Provide technical, operational, and administrative support to BWXT Y-12 Network Manager and BWXT Y-12 Radio Manager in the transition of the Y-12 National Security Complex radio system and radio equipment to the narrowband frequencies required by federal law. Coordinate and schedule services to insure all VHF radios are replaced with narrowband equipment before January 1, 2005. Coordinate and schedule services to insure all UHF radios and the Y-12 National Security Complex trunking system are replaced with narrowband equipment before January 1, 2008. Work with impacted BWXT Y-12 organizations to transition to narrowband equipment.

15. Provide technical evaluations of wireless equipment and services for the Y-12 National Security Complex network management. Assist users with requests and proposals for wireless communications services.

16. Assist BWXT Y-12 management in regulating wireless communications equipment and services on the Y-12 National Security Complex to insure compliance with corporate, computer security, network, and other policies directed by NNSA.

Table 8. Summary of BWXT Y-12 radio equipment

Conventional Desktop	1
Conventional Mobile	15
Conventional Portable	226
Conventional Repeaters	12
Trunked Desktop	39
Trunked Mobile	102
Trunked Portable	1413
Trunked Repeaters	7
Trunked RF Modem	6

3.2.15.2.5 General Voice and Wireless Services Support

The Contractor shall:

1. Provide configuration management for all voice and wireless systems software, hardware, and media.

2. Work with USN Manager and customers to process wireless technology requests, including processing requests for wireless devices, researching new technologies, tracking requests, and interacting with vendors.

3. Develop procedures and processes concerning voice and wireless services as requested.

4. Provide recommendations for infrastructure and process improvements, architectures and standards improvements, and new technologies applicable to the PWS that would reduce operational costs and/or significantly improve the level of service.

5. Provide performance analysis and optimize resource utilization. Monitor workload and system performance information. Initiate routine upgrades of voice and wireless system hardware and software, and recommend upgrades for performance optimization to support BWXT Y-12 workload projections. Recommend voice and wireless system consolidations and shutdowns.

6. Provide oversight of voice and wireless system hardware and software maintenance agreements necessary to support the operations of the system equipment and software. This activity involves interactions with vendors, procurement, and finance personnel. Specific activities include, but are not limited to, voice and wireless system hardware and software inventorying, funds management, procurement recommendations, upgrades, extensions, and compliance.

7. Support Y-12 National Security Complex budget development for the services noted in this PWS on an annual basis in line with BWXT Y-12 schedules, formats, and procedures. Responses to BWXT Y-12 inquiries and questions shall be documented and completed in a timely manner.

3.2.15.3 Performance Requirements

1. Services provided by the Contractor shall be available, timely and meet quality expectations.

2. The Contractor shall meet or exceed resource utilization, system performance, security compliance, problem notification, and established resolution turnaround time requirements.

3.2.16 Computer Maintenance Services for 1099 Commerce Park

3.2.16.1 Introduction

The Contractor shall provide computer maintenance support services to BWXT Y-12 for the 1099 Commerce Park Facility and other remote office locations for setup, installation, maintainance, and repair of computing equipment, including the various networks, communications infrastructure, systems and other related services.

Services shall be performed at the 1099 Commerce Park Facility. Approximately 230 desktop users and approximately 20–30 servers are located in the facility.

3.2.16.2 Services

The Contactor shall:

1. Provide repair services for personal computer (PC) workstation components and associated computers and peripherals. Repair procedures may involve the following activities: troubleshooting, testing to confirm diagnosis, installation of replacement parts, and testing to confirm satisfactory performance of the component or system. Work shall be prioritized and scheduled by Y-12's 1099 Commerce Park Computer Maintenance Manager (or designated representative) on a daily basis. The following computing components may require service:

   - hard drives and CD-ROM drives ,
   - motherboards,
   - power supplies,
   - memory,
   - video and sound cards,
   - network interface cards,
   - input devices (keyboard, mouse, etc.),
   - peripherals, including laser and inkjet printers and plotters,
   - related supporting equipment, such as uninterruptible power supplies (UPSs) (with replaceable batteries), and
   - related network and communications infrastructure equipment.

2. Provide occasional "on-call" repair services on an expedited basis to return an identified component to service as rapidly as practical. Network components that may require expedited service include file servers, hard drives, RAID Arrays (Small Computer Software Interface (SCSI)), and multi-processor systems, network switches, and other related computing components.

3. Provide general computer user support to address BWXT Y-12 computing requirements. The Contractor shall resolve user problems regarding the various networks, communications infrastructure, systems, and protocols

4. Provide a technical competency to assist staff in identifying equipment to meet computing requirements and to build, upgrade, and/or repair computing equipment and peripherals.

5. Provide support for conferences and workshops held at the facility and other off-site locations, as required. The Contractor shall setup and operate audiovisual systems and related computing peripheral equipment.

6. Assist the facility manager and personnel in relocating and/or disposing of computing equipment. The Contractor shall perform such functions as moving and setting up equipment, sanitizing equipment before it is processed as surplus, and assist with building security and related systems, and including repair and installation of fiber optic, twisted pair (CAT-5, CAT-5e, and CAT-6) data communications networks.

7. Provide services at various work locations throughout the United States and abroad. The principal location for the computing services provided by this agreement is the 1099 Commerce Park Facility. However, BWXT Y-12 maintains remote offices and provides technical assistance to sponsoring organizations through the Complementary Work Program. Travel shall be arranged by the Contractor and reimbursed by BWXT Y-12 utilizing its travel policy.

8. Repair work described in this service is considered non-hazardous. All activities performed are to be conducted in accordance with generally accepted lock out/tag out practices for working with electricity and electrical components related to PCs to insure the safety of worker(s) and the protection of equipment. No cleaners or solvents are to be used at BWXT Y-12 work locations.

9. Track manufacturer warranties applicable to computing equipment and pursue remedies available from the manufacturer before initiating any repairs that may void the warranty.

10. Work assignments shall be performed for a variety of contractors, including tenants of the facility from several organizations, and a variety of Complementary Work for Others contractors. The Contractor, with assistance from the 1099 Commerce Park Computer Maintenance Manager, is responsible for identifying the specific and applicable work breakdown structure (WBS) number for each work assignment. The personnel shall use BWXT Y-12 Absence Payroll Labor Utilization System (APLUS) to record time by WBS for work assignments.

11. Computing equipment or components may only be removed from 1099 Commerce Park with the specific authorization of the 1099 Commerce Park Computer Maintenance Manager and with proper documentation required by BWXT Y-12 procedures.

12. Provide continuing training to accomplish work assignments and to remain current with computer technology.

13. Provide support from 7 a.m. – 5 p.m. Monday through Friday. A minimum of two (2) employees is required during the core hours 9 a.m. – 3 p.m. During lunch periods, one employee is acceptable for a period of up to one hour. Off-shift work hours may be

scheduled by BWXT Y-12 to accomplish network-related and other activities with minimal disruption of service, to expedite a repair or to reduce backlog.

14. Provide additional support upon request, such that the requested services are available during personnel absences or to balance workload peaks.

15. Provide qualified personnel to perform the following:

    15.1. diagnostics, repairs, and upgrades on state-of-the art personal computing equipment and peripherals;

    15.2. accelerated training on new computing equipment technologies and equipment;

    15.3. servicing a variety of computer processors (e.g., Pentium, Pentium Pro, Pentium II, Pentium III, and AMD), motherboard forms (AT and ATX), and random access memory (SDRAM, SIMMs, and DIMMs);

    15.4. installation, configuration, and troubleshooting of Microsoft operating systems (Windows NT, 2000, 2003, and XP) in stand-alone and networked configurations;

    15.5. installation and support of CISCO, Extreme and networking hardware;

    15.6. installation and support of a variety of computer brands (Dell, Sun, Southwind, Silicon Graphics Inc – SGI, Compaq, etc.); and

    15.7. installation, configuration, and troubleshooting of fiber optic, twisted pair, and thin wire data communications networks.

3.2.16.3 Performance Requirements

1. The quality of work expected in repairing all equipment is to bring the affected item into conformance with its as-manufactured operating condition, except when an upgraded component is authorized to be substituted for a failed component. The repair shall be deemed to be satisfactorily completed when the item is accepted and returned to service or inventory.

2. Services provided by the Contractor shall be available, timely and meet quality expectations.

3.2.17 SAP Support

3.2.17.1 Introduction

The Contractor shall provide technical support for new module/product implementation, current development, and ongoing maintenance of the SAP system.

BWXT Y-12 is currently operating multiple instances of SAP software in support of its Business and Human Resources systems. SAP has replaced a number of the existing Finance, Project Management, Acquisition, and Human Resource systems previously in use at Y-12. SAP Version 4.6C is the current production release at Y-12. There are 3500 users of the system at Y-12.

The SAP application and environment characteristics include:

1. Tools: Oracle, C++, ABAP, SAP
2. Web Development: Java, JavaScript, HTML
3. Processors/Environment: SUN Solaris, NT
4. Encompasses all business areas
5. Complex business logic
6. Complex interface and integration
7. Complex technical attributes

3.2.17.2 Services

Services include SAP application programming support and UNIX and NT system support as described below.

3.2.17.2.1 SAP Development and Maintenance Support

The Contractor shall provide technical support for ongoing development and maintenance of the SAP system, resolution of technical problems, and implementation of technical solutions necessary to maintain the basic functionality and integrity of the system.

Note: While it is currently estimated that approximately 15 technical developers shall be involved in the ongoing development and maintenance of the SAP system, this technical support shall be a mixture of contract, BWXT Y-12 staff, and consulting resources.

3.2.17.2.2 SAP Operations Support

The Contractor shall provide technical support for ongoing systems operation and maintenance and resolution of technical problems necessary to maintain the basic functionality and integrity of the system.

Note: While it is currently estimated that approximately five (5) technical employees will be involved in ongoing maintenance and operation of SAP functional modules and the Basis operating system, this technical support shall be a mixture of contract, BWXT Y-12 staff, and consulting resources.

3.2.17.2.3 SAP Pension Support

The Contractor shall provide technical support for ongoing development and maintenance of the SAP Pension system, resolution of technical problems, and implementation of technical solutions necessary to maintain the basic functionality and integrity of the system.

3.2.17.3 Performance Requirements

1. Qualified personnel shall provide support services as outlined for the SAP.

2. Services provided by the Contractor shall be available, timely and meet quality expectations.

3.2.18DOE IT Support Services

3.2.18.1 Introduction

The Contractor shall provide technical support services for DOE/ORO.

3.2.18.2 Services

3.2.18.2.1 General IT Support for DOE

The Contractor shall provide IT support services, for a variety of tasks in areas such as: UCAMS account management; NT domain configuration and support; infrastructure support relating to security, networking, and internet access.

Provide operation and management support for the Department of Energy Business Network (DOEBN) wide area network node for Oak Ridge. Work consists of managing the local DOEBN router node and performing coordination functions between the project team at Germantown MD, and Oak Ridge. This includes DOEnet router support and transition to the new DOEnet ATM network.

Provide requested software development support.

3.2.18.2.2 DOE Radio Support

Coordinate radio administration functions on the DOE Oak Ridge Reservation (ORR) for DOE.

Monitor and provide technical assistance concerning issues relative to the ORR radio systems as requested by Oak Ridge Operations (ORO) Information Resources Management Division (IRMD).

3.2.18.3 Performance Requirements

Services provided by the Contractor shall be available, timely and meet quality expectations.