Addendum III

STATEMENT OF WORK

FOR THE

DEFENSE RESEARCH

ENGINEERING NETWORK (DREN)

CONTRACT

February, 2001

TABLE OF CONTENTS

1.0 BACKGROUND 1-1

1.1 PURPOSE AND OBJECTIVES 1-1

1.2 THE DREN PROGRAM 1-1

1.3 CONTRACT SCOPE 1-2

1.3.1 DREN Customers 1-2

1.3.2 Customer Network Objectives 1-2

1.4 FUNCTIONAL COMMUNITIES TO BE SUPPORTED BY DREN SERVICES 1-2

1.4.1 The S&T and T&E Communities 1-3

1.4.2 The M&S Community 1-3

1.5 GENERAL DESCRIPTION OF THE REQUIREMENTS 1-4

1.6 TERMS AND DEFINITIONS USED IN THIS DOCUMENT 1-4

1.6.1 Service Delivery Point 1-4

1.6.1.1 SDP Service. 1-5

1.6.1.2 SDP Sustained Data Rate 1-5

1.6.1.3 SDP Peak Data Rate. 1-5

1.6.2 SDP Site 1-5

1.6.3 Permanent Virtual Circuit (PVC) 1-5

1.6.4 Switched Virtual Circuit (SVC) 1-5

1.6.5 Soft Permanent Virtual Circuit (SPVC) 1-5

1.6.6 Current Version 1-5

1.6.7 Customer Premise Equipment 1-5

1.6.8 Paragraph References 1-5

2.0 APPLICABLE DOCUMENTS 2-1

2.1 STANDARDS 2-1

2.1.1 Required Standards 2-1

2.1.2 Sources of Standards 2-3

2.1.3 Standards Provided as Reference 2-3

2.2 SECURITY REFERENCES 2-3

2.2.1 Executive Documents 2-3

2.2.2 Department of Defense Documents 2-3

2.2.3 Computer Security Documents 2-3

2.2.4 Operational Security Documents 2-4

2.2.5 Personnel Security Documents 2-4

3.0 REQUIREMENTS 3-1

3.1 PROGRAM MANAGEMENT 3-1

3.1.1 Program Management Office 3-1

3.1.2 Project Management Planning and Control 3-2

3.1.3 Progress Reporting 3-2

3.1.4 Quarterly Project Management Reviews 3-2

3.1.5 Annual Planning and Design Review 3-2

3.1.5.1 Review 3-2

3.1.5.2 Annual DREN Users Conference 3-3
3.2 IMPLEMENTATION & TRANSITION 3-3
3.2.1 Planning 3-3
3.2.1.1 Transition Planning (Phase I) 3-4
3.2.1.2 Transition Planning (Phase II) 3-4
3.2.1.3 Content of Comprehensive Implementation & Transition Plan 3-5
3.2.2 Implementation & Transaction Actions 3-7
3.2.2.1 Phase I Actions 3-7
3.2.2.2 Phase II Actions 3-7
3.3 STEADY-STATE NETWORKING ACTIONS 3-7
3.3.1 Install, Modify, Terminate, and Restore SDPs 3-7
3.3.1.1 SDP Plans 3-7
3.3.1.2 Alteration, Installation, and Modification 3-9
3.3.1.3 Acceptance Procedures 3-10
3.3.1.4 Termination/Restoration 3-10
3.3.2 Disaster Recovery and Contingency 3-10
3.3.3 Services at SDPs That Perform Gateway Functions 3-10
3.4 DIGITAL DATA TRANSFER SERVICES 3-11
3.4.1 SDP Characteristics 3-11
3.4.1.1 SDP Services 3-12
3.4.1.2 SDP Data Transfer Rates 3-13
3.4.2 SDP Functional Requirements 3-14
3.4.2.1 SDP and VC Availability Requirements 3-15
3.4.2.2 PVC Failsafe 3-16
3.4.2.3 IP Performance/Packet Loss 3-16
3.4.3 Network-Related SDP Performance Requirements 3-17
3.4.4 Contractor Verification of Services 3-18
3.4.4.1 Individual SDP Test 3-18
3.4.4.2 Collective SDP Test 3-18
3.4.4.3 Government Verification of Services 3-19
3.4.5 Local Connectivity from SDP Sites to Secondary Sites 3-19
3.5 EVOLUTION OF EXISTING SERVICES 3-19
3.5.1 Technology Insertion 3-20
3.5.2 Upgrades 3-20
3.5.3 Government versus Contractor Initiated Proposals 3-21
3.5.3.1 Government Initiated 3-21
3.5.3.2 Contractor Initiated 3-21
3.6 NETWORK MANAGEMENT 3-21
3.6.1 Network Supervision and Maintenance 3-21
3.6.2 Fault Management 3-21
3.6.2.1 Fault Management at Network Level 3-22
3.6.2.2 Problem and Fault Isolation – Type A IP Packet-based SDP Services 3-22
3.6.2.3 Problem and Fault Isolation- Type B ATM Cell-based SDP Services 3-22
3.6.2.4 Problem and Fault Isolation- Type C Lightwave SDP Services 3-23
3.6.2.5 Problem and Fault Isolation – SDP Utilized as Gateways 3-24
3.6.3 Performance Management 3-24
3.6.3.1 Performance Measurement and Validation – TYPE A IP Packet-Based SDP Services 3-24

3.6.3.2 Performance Measurement and Validation – Type B ATM Cell-based SDP Services 3-24
3.6.3.3 Performance Measurement and Validation – Type C Lightwave SDP Services 3-25
3.6.4 Configuration Management 3-25
3.6.5 Network Management Reporting 3-26
3.7 CUSTOMER CARE 3-27
3.7.1 Service Provisioning 3-27
3.7.1.1 Service Requests and Task Orders 3-27
3.7.1.2 Provisioning of Service Requests and Task Orders 3-28
3.7.1.3 Service Request and Task Order Tracking 3-29
3.7.2 Service and Problem Management 3-30
3.7.2.1 Help Desk 3-30
3.7.2.2 Customer Problem Management 3-31
3.7.2.3 Record Keeping 3-32
3.7.3 Customer Care Data and Reports 3-33
3.7.4 Accounting Management 3-34
3.7.5 Customer Support and Instructional Services 3-34
3.7.5.1 Instructional Services 3-34
3.7.5.2 Technical Support Services 3-34
3.7.5.3 Telecommunications-Related Support 3-35
3.7.5.4 Engineering Studies 3-35
3.8 CONTRACT PHASE-OUT 3-35
3.8.1 Planning and Engineering Support 3-35
3.8.1.1 Development of Contract Phase-Out Transition Plan 3-35
3.8.1.2 Updating, Validating, and Transferring of Support Documentation 3-36
3.8.2 Phase-Out 3-36
4.0 SECURITY 4-1
4.1 SECURITY SERVICE REQUIREMENT 4-1
4.1.1 Access Control 4-2
4.1.2 Identification and Authentication 4-2
4.1.3 Confidentiality and Integrity 4-3
4.1.4 Physical Security 4-3
4.1.5 Personnel Security 4-4
4.2 CERTIFICATION AND ACCREDITATION SUPPORT 4-4
4.2.1 System Security Authorization Agreement 4-5
4.2.2 Security Test and Evaluation Plan 4-5
4.3 SECURITY OPERATIONS 4-5
4.3.1 Network Management Data 4-5
4.3.2 Access By Authorization Levels 4-6
4.3.3 Service Protection 4-6
4.3.4 Security Incident Reporting 4-6
4.3.5 Security Vulnerabilities 4-7
4.3.6 Security Audit Reporting 4-7
4.3.7 Continuity of Operations 4-7
4.3.8 Site-specific Security Requirements 4-8
5.0 DELIVERABLES 1

1. BACKGROUND

1.0 BACKGROUND

1.1 PURPOSE AND OBJECTIVES

The purpose of this procurement is to provide state-of-the-art Wide Area Networking (WAN) services to support the Department of Defense (DoD) High Performance Computing Modernization Program (HPCMP) and DoD users in various technical communities. As part of the HPCMP, the overall Government networking capability that links these users together is called the Defense Research Engineering Network (DREN). Current networking capability is being provided under the DREN Inter-site Services Contract (DISC), which expires in July 2001. This procurement will enable continuation of the DREN network capability under a follow-on contract.

1.2 THE DREN PROGRAM

The HPCMP is chartered to establish, provide, and maintain leading edge High Performance Computing (HPC) capability for scientists and engineers engaged in DoD science and technology, test and evaluation, and research and development missions. The DREN, an initiative of the HPCMP, provides the WAN services that enable high-speed connectivity among the sites housing the DoD scientists, engineers, and HPC resource centers.

The DREN is a sophisticated, robust DoD communications network that incorporates the best operational capabilities of both the DoD and the commercial telecommunications infrastructure. DREN has become DoD's premier long-haul communication service provider for the HPC community.

The DREN enables over 6000 scientists and engineers at defense laboratories, test centers, universities, and industry sites throughout the United States to use HPCMP computing resources. Of these, over 3000 are remote customers, working in locations outside the supercomputer sites from which they obtain services. The DREN provides gateways to existing military and civilian networks, allowing access to the program's resource centers from Contractor and university facilities.

The networking services of DREN are currently provided by a virtual WAN built on a public communications network supplied by AT&T as part of the DISC. The DISC, awarded to AT&T on July 16, 1996, expires July 10, 2001. The DISC provides digital data transfer services between defined service delivery points (SDP) that comprise the DREN. SDPs are specified in terms of their bandwidth requirements and the physical and transport protocols that they must support. The follow-on DREN contract will provide networking services after expiration of the existing contract.

The DREN provides interoperable asynchronous transfer mode (ATM) and Internet Protocol (IP) services for video, audio, imaging, and digital data and connects to other research and academic networks at Federal Internet Exchanges and Metropolitan Area Exchanges. The network links customer sites to DoD's four Major Shared Resource Centers (MSRC) and 17 Distributed Centers (DC). The DREN has a mix of more than 70 ATM and IP sites. (See Attachment B – DREN Sites). The current network provides Digital Service 3 (DS-3) through

OC-12 connectivity. The HPCMP plans to continue to upgrade DREN to establish connectivity at higher speeds.

The Defense Information Systems Agency Information Security Program Management Office has validated DREN for Sensitive But Unclassified (SBU) information.

1.3 CONTRACT SCOPE

The scope of this contract encompasses state-of-the-art WAN digital transfer and related services to support DREN customers.

1.3.1 DREN Customers

The Contractor shall support DREN customers. The DREN customers are currently located at DoD, other Government, academic, and Contractor sites in all 50 states. Future DREN customers may be located in CONUS, Hawaii, Alaska, Puerto Rico, Guam, other U.S. territories, and the Bahamas. DREN customers are from the following DoD communities:

a) Science and Technology (S&T);

b) Test and Evaluation (T&E);

c) Modeling and Simulation (M&S);

d) Ballistic Missile Defense Organization (BMDO); and

e) Defense Threat Reduction Agency (DTRA).

1.3.2 Customer Network Objectives

The network services shall support the following objectives of the S&T, T&E, BMDO, DTRA, and M&S communities:

a) Effectively pooling resources and encouraging collaboration;

b) Real-time visualization and modeling and simulation;

c) Rapid access to multi-media libraries and large distributed computational resources using meta-computing approaches such as Globus and Legion;

d) Linking DREN customers to the Internet; national networks such as National Science Foundation's vBNS, Energy Sciences Network (ESNet) ; and various R&D network testbeds such as the Internet2 Abilene project.

e) Connectivity from the user's desktop to HPC capabilities, databases, libraries and other users at data rates of Gigabits per second (Gbps).

1.4 FUNCTIONAL COMMUNITIES TO BE SUPPORTED BY DREN SERVICES

The DoD requires that the DREN WAN services provide direct support to five separate functional "communities" of customers: DoD S&T community, the DoD T&E community, the

BMDO community, the DTRA community, and the DoD M&S community. These communities have somewhat different areas of interest, different sources of funding, different internal programming procedures, and independently derived mission objectives and priorities. They share a common need for support by HPCMP computing resources and for WAN data transport support that will be provided by the DREN services. The sites to be connected by DREN services may be at virtually any point in the Continental United States (CONUS), Alaska, Hawaii, Puerto Rico, Guam, and other U.S. territories. Over 3000 of the approximately 6000 customers are remote customers, working at locations other than DoD supercomputer sites that provide HPCMP services.

The data transport service requirements of DREN are derived from customer requirements for remote computer operations and from the need to engage in collaborative initiatives in distributed and interactive environments. The DREN customers employ applications that require enormous computing capabilities. The corresponding network traffic to support these HPC capabilities is projected to require greater than OC-12 connectivity within 3 years at the most demanding sites.

1.4.1 The S&T and T&E Communities

The base of the S&T and T&E work of the DoD is increasingly dependent on using computers and software to replace physical experiments and direct measurement. The users and the computers are distributed geographically all over the country. The networks that connect system components are the enabling links that let it all work. In all cases today, users who are remote from their computers and data sources must operate differently from those who have local resources. The difference is in the time required to transmit data between the separated sites. DREN must transmit data at rates that will minimize these effects of separation and enable each user and groups of researchers around the country to work together more effectively as if they were collocated with one another.

1.4.2 The M&S Community

Projects within the M&S community are developing similar requirements for network speeds and computational resources. The demands on DREN from this community will grow in parallel with those of the HPC customers.

Distributed modeling and simulation is a method of building large, complex simulations by combining simulations of pieces of the problem. Thus merging individual simulations from remote sites that separately model aircraft, weapons, ground forces, trucks, tanks, and ships might produce a battlefield scenario. This approach enables more complex simulations than could be achieved at any single site. The customer requirements for the interactive distributed simulation are influenced strongly by the need to perform interactive visualization.

The research done in this community is leading to the application of powerful computers to support system concept evaluation, system design, training, testing, and tactics planning and evaluation. The use of simulations in these areas shows the potential for significantly improved overall results and dramatic savings of time, money, and personnel involvement. The aspect of the distributed M&S work that is relevant to DREN is the required interaction of research sites that are geographically separated throughout the country. These separated sites must be networked together. The detailed requirements for precise control of the data interchanges

among the participants can put unique constraints on the network design and operation. The need for interactive visualization often mandates extremely high bandwidth and near error-free data transmission between sites.

1.5 GENERAL DESCRIPTION OF THE REQUIREMENTS

The requirements set forth in this Statement of Work (SOW) are for commercial state-of-the-art WAN digital data transfer services and related management and support services, as listed below:

a) Establishment of an initial performance capability by installing a set of SDPs and establishing the operational environment (See Section 1.6.1 for the definition of the term SDP);

b) Provision of concurrent digital data transfer service between and among SDPs;

c) Performance of the actions needed to implement changes to the set of active SDPs;

d) Performance of technical support (such as engineering technical support, technical studies, and technology insertion) and instructional service related to the customers' present or future operational environment being supported by Contractor-provided services; and

e) The DREN network is not required to provide any encryption capabilities within the local site infrastructures (customer side of the interface). However, the DREN will be protected from breach of the network (that is illegal tapping, leaking, or diversion of data) and provide confidentiality for transmitting DoD data at the SBU level.

Only commercial items, as defined in FAR Clause 52.202-1, Definitions (October 1995) shall be used to satisfy the requirements of this contract.

1.6 TERMS AND DEFINITIONS USED IN THIS DOCUMENT

Definitions and meanings of data processing, data communications, and information systems terms used in this SOW which are not defined herein shall be interpreted in accordance with FIPS Publication 11-3, Guideline: American National Dictionary for Information Processing Systems.

1.6.1 Service Delivery Point

An SDP shall be defined as a combination of physical, electrical/optical, functional, procedural, protocol, and service characteristics that establish an interface between the Contractor's network and Government-designated customer premise equipment (CPE). There shall be a single SDP deployed for each DREN site. For a given SDP the Government will choose one or more hardware interfaces between the SDP and the Government site CPE, and select sustained and peak data transfer rates for all user traffic using a given SDP to reach the DREN. Each SDP shall be capable of supporting multiple protocols and services (e.g., ATM, IP). SDPs located at Network Access Points (NAP), Metropolitan Area Exchanges, and GigaPOPs will also provide network gateway services. SDP services providing the CPE interfaces will be

defined in terms of their hardware interface, and by their sustained and peak throughput rates. The Contractor shall provide service via an SDP that defines the demarcation between Contractor and Government responsibilities. There are three additional definitions related to SDPs:

1.6.1.1 ***SDP Service:*** An SDP Service, or Service," shall be defined as a specific packet, cell, or other service defined in 3.4.1 at the SDP and which Government CPE connects to interfaces within the SDP that support that service in order to access the DREN.

1.6.1.2 ***SDP Sustained Data Rate:*** The SDP sustained data rate shall be defined as the average two-way data transfer rate for Government data traffic between an SDP and the DREN, aggregated across all SDP Services configured at that SDP

1.6.1.3 ***SDP Peak Data Rate:*** The SDP peak data rate shall be defined as the peak or maximum two-way data transfer rate for Government data traffic between an SDP and the DREN, aggregated across all SDP Services configured at that SDP.

1.6.2 SDP Site

An SDP Site shall be defined as the Government, commercial, or academic installation or facility in which an SDP is established.

1.6.3 Permanent Virtual Circuit (PVC)

A PVC is a provisioned virtual connection that stays up until taken down as defined in relevant ATM Forum Standards.

1.6.4 Switched Virtual Circuit (SVC)

A SVC is a logical circuit set up on demand by user signaling that stays up for the duration of the session as defined in relevant ATM Forum Standards.

1.6.5 Soft Permanent Virtual Circuit (SPVC)

An SPVC is set up by invoking SPVC call set up procedures and stays up until it is taken down as defined in relavant ATM Forum Standards .

1.6.6 Current Version

“Current version” shall refer to the most recently ratified version of the referenced standard available at any instant in time throughout the life of the contract.

1.6.7 Customer Premise Equipment

CPE refers to Government-designated equipment (including cabling) that is directly attached to an SDP. It does not refer to Contractor-provided equipment used to deliver service at, or as a part of, an SDP.

1.6.8 Paragraph References

Unless otherwise indicated, all references of the form "paragraph x" are to paragraphs within this SOW.

2. APPLICABLE DOCUMENTS

2.0 APPLICABLE DOCUMENTS

2.1 STANDARDS

2.1.1 Required Standards

a) ATM User-Network Interface Specification, Version 4.1, The ATM Forum;

b) The B-ISDN Intercarrier Interface (B-ICI), Version 2.0, The ATM Forum;

c) ATM Traffic Management Specifications, Version 4.1, The ATM Forum;

d) Bellcore GR 253-CORE SONET Transfer system: Common Generic Criteria;

e) Multimedia Over Packet, H.323, ITU-T;

f) Internet Protocol Standard 1 (STD1) Specification, RFC 2700(or current version)

g) Internet Protocol Version 6 (Ipv6) Specification, RFC 2460;

h) Security Architecture for the Internet Protocol, RFC 2401;

i) Internet Protocol Security (IPSec) Document Roadmap, RFC 2411; and

j) Classical IP and ARP Over ATM, RFC 2225.

k) ANSI T1.105, Telecommunications - Synchronous Optical Network (SONET) Basic Description Including Multiplex Structure, Rates and Formats (ATIS) (Revision and Consolidation of ANSI T1.105-1991 and ANSI T1.105A-1991), 1995.

l) ANSI T1.107 Digital Hierarchy - Formats Specifications, 1995.

m) ANSI T1.117, Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode Short Reach), 1991.

n) ATM Forum, af-ilmi-0065.000, Integrated Local Management Interface (ILMI) Specification, Version 4.0, September 1996.

o) ATM Forum, af-pnni-0055.000, Private Network to Network Interface (PNNI) Specification, Version 1.0, March 1996.

p) ATM Forum, af-sig-0061.000, ATM UNI Signaling Specification, Version 4.0, July 1996.

q) ATM Forum, af-tm-0056.000, Traffic Management Specification, Version 4.0, April 1996.

r) ATM Forum, af-uni-0010.002, ATM UNI Specification V3.1, September 1994.

s) ATM Forum, af-vtoa-0078.000, Circuit Emulation Service Interoperability Specification, Version 2.0, January 1997.

t) ATM Forum,af-pnni-0066.000, PNNI Specification, Version 1.0 Addendum (Soft PVC MIB), September 1996.

u) IEEE 802.3 Standards

v) IETF Informational RFC 1770, IPv4 Option for Sender Directed Multi-Destination Delivery, 28 March 1995.

w) IETF RFC-1305, Network Time Protocol (Version 3) Specification, Implementation, and Analysis, March 1992.

x) IETF RFC 1483, Routed PVC Support

y) IETF RFC-1514, Host Resources MIB, September 1993.

z) IETF RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 1993.

aa) IETF RFC-1738, Uniform Resource Locators (URL), 20 December 1994.

bb) IETF RFC-1757, Remote Network Monitoring Management Information Base, (RMON Version 1), February 1995.

cc) IETF RFC-1771, A Border Gateway Protocol 4 (BGP-4), 21 March 1995.

dd) IETF RFC-1772, Application of the Border Gateway Protocol in the Internet, March 1995.

ee) IETF RFC-1808, Relative Uniform Resource Locators, June 1995.

ff) IETF RFC-1812, Requirements for IP Version 4 Routers, 22 June 1995.

gg) IETF RFC-1850, Open Shortest Path First (OSPF) Version 2 Management Information Base, November 1995.

hh) IETF RFC-2001, TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, January 1997.

ii) IETF RFC-2131, Dynamic Host Configuration Protocol, March 1997.

jj) IETF RFC-2616, Hypertext Transfer Protocol (HTTP)/1.1, June 1999.

kk) IETF Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987.

ll) IETF Standard 15/RFC-1157, Simple Network Management Protocol (SNMP), May 1990.

mm) IETF Standard 16/RFC-1155/RFC-1212, Structure of Management Information, May 1990.

nn) IETF Standard 17/RFC-1213, Management Information Base, March 1991.

oo) IETF Standard 33/RFC-1350, The TFTP Protocol (Revision 2), July 1992, to be used for initialization only.

pp) IETF Standard 37/RFC-826, An Ethernet Address Resolution Protocol, November 1982.

qq) IETF Standard 41/RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984.

rr) IETF Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112, Internet Protocol, September 1981.

ss) IETF Standard 50/RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994.

tt) IETF Standard 54/RFC-2328, Open Shortest Path First Routing Version 2, April 1998.

uu) IETF Standard 6/RFC-768, User Datagram Protocol (UDP), 28 August 1980.

vv) IETF Standard 7/RFC-793, Transmission Control Protocol, September 1981.

ww) IETF Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983.

xx) ITU-T H.323 Multimedia over Packet

yy) ITU-T I.363.1, B-ISDN ATM Adaptation Layer Specification: Type 1 ATM Adaptation Layer (AAL1), August 1996.

zz) ITU-T I.363.5, B-ISDN ATM Adaptation Layer Specification: Type 5 ATM Adaptation Layer (AAL5), August 1996.

aaa) MIL-STD-2045-47001B, Connectionless Data Transfer Application Layer Standard, 20 January 1998.

2.1.2 Sources of Standards

a) ATM Forum;

b) Internet Engineering Task Force (IETF);

c) International Telecommunications Union (ITU);

d) American National Standards Institute (ANSI) ; and

e) Institute of Electrical and Electronic Engineers (IEEE).

2.1.3 Standards Provided as Reference

The following additional standards are provided as reference.

a) Multiprotocol Over ATM (MPOA), Version 1.0, The ATM Forum; and

b) Resource ReSerVation Protocol (RSVP), RFC 2205.

2.2 SECURITY REFERENCES

2.2.1 Executive Documents

a) Executive Order12958, "Classified National Security Information;"

b) Public Law 99-508, "Electronic Communications Privacy Act of 1986;"

c) Public Law 100-235, "The Computer Security Act of 1987;"

d) OMB Circular no. A-130, "Management of Federal Information Resources;" and

2.2.2 Department of Defense Documents

a) DoD Instruction 5200.40, "Defense Information Technology Security Certification and Accreditation Process;"

2.2.3 Computer Security Documents

a) DoD Directive 5200.28, "Security Requirements for Automated Information Systems;"

b) Federal Information Processing Standards Publications (FIPS PUBS) Security Requirements for Cryptographic Modules (FIPS PUB 140-1)

2.2.4 Operational Security Documents

a) Deputy Secretary of Defense Memorandum, DoD Information Assurance Vulnerability Alert (IAVA) ; and

b) Joint Chief of Staff Memorandum CM-510-99, Information Operations Conditions

2.2.5 Personnel Security Documents

a) DoD Regulation 5200.2-R, "Personnel Security Program Regulation;"

3. REQUIREMENTS

3.0 REQUIREMENTS

The Contractor shall deliver the services set forth in this SOW, pursuant to issuance of task orders. The Contractor, acting independently, and not as an agent of the Government, shall furnish all management, personnel, equipment, software, services, travel, and other items necessary to successfully deliver the indicated services. DREN WAN services shall be delivered to Government designated locations referred to as SDP Sites. The Contractor shall implement and operate the services required in this SOW. The Contractor shall comply with the standards identified in Section 2.0 in performance of the services provided under this SOW.

3.1 PROGRAM MANAGEMENT

The Contractor shall furnish all personnel, materials, facilities, and services required to provide DREN Services in accordance with this SOW. The Contractor shall provide planning, direction, coordination, and control necessary to accomplish all requirements contained in this contract. The Contractor shall determine and establish the project organization that shall provide overall management of the contract work. The Contractor shall designate a key individual who is responsible for the cost, schedule, and technical performance on the contract and who will serve as a primary point-of-contact for both management and technical matters. In addition, the Contractor shall conduct program review meetings and produce documentation to keep the Government informed on the status of all tasks.

References to "the Government" in this SOW shall be interpreted to mean an authorized Government representative as designated by the Contracting Officer.

3.1.1 Program Management Office

The Contractor shall establish and operate a Program Management Office (PMO) to provide management and operations support to the Government and to act as a single point of contact for Government management and administration of the DREN contract. In addition the PMO shall provide a central coordination point(s) for:

a) All DREN problems not resolved at the local site; and

b) Government-initiated DREN testing activities.

The minimum normal business hours for the PMO shall be Monday through Friday from 8:00 AM to 5:00 PM Eastern Time (ET). The PMO shall be established upon contract award and should be fully operational within 30 business days following contract award. The PMO shall coordinate with designated Government representatives on an ongoing basis and act as a source of information and assistance for this contract.

The Contractor's PMO shall be located within 25 miles of the DREN/HPCMP Management Office located in Arlington, Virginia.

3.1.2 Project Management Planning and Control

The Contractor shall develop a course of action and schedule for meeting the requirements set forth in this contract. The Contractor shall include in all such planning activities: risk management practices, procedures, and tools that will be used to control resources; schedules and procedures for developing the reports, and providing the data required under the contract.

3.1.3 Progress Reporting

The Contractor shall monitor and evaluate the DREN activities and report the status to the Government. The Contractor shall monitor and report on the efficiency and effectiveness of transition on a monthly basis. In addition, the Contractor shall attend weekly status meetings on the progress of transition until all existing DREN SDPs have been transitioned to this follow-on contract. After completion of transition, the Contractor shall develop the progress reports on a quarterly basis. The quarterly progress report will identify significant activities, problems, and accomplishments during the preceding three months.

3.1.4 Quarterly Project Management Reviews

The Contractor shall conduct regular quarterly reviews until Phase II transition is complete and subsequently upon Government request to address the current status of technical and programmatic progress. The Government will notify the Contractor at least 30 days in advance of a request to conduct a review unless operational and maintenance issues require meetings on an immediate basis. Each review shall focus on achievements since the last review, conduct and success of risk management activities, unresolved issues, action items, and problems. The Contractor shall support preparation for and execution of the meetings by:

a) Assisting in the development of agendas by identifying issues, problems, and/or opportunities to improve services and systems;

b) Participating in subcommittees, working groups, or other planning and support activities identified in the coordination meetings; and

c) Generating meeting minutes.

These review meetings shall take place at a location determined by the Government.

3.1.5 Annual Planning and Design Review

3.1.5.1 Review

The Contractor shall conduct an annual review meeting to address the status of available contract services and to assess the potential for changes that can enhance technology, reduce costs, improve end-user services, or enhance administrative and management systems for the DREN. The Contractor shall prepare and present analyses and data to support the Planning and Design Review including, as necessary, the following:

a) Current network design and engineering data;

b) Growth analyses and resource allocations;

c) Planned transmission network growth;

d) Trend analyses and projections;

e) Security measures and potential improvements;

f) Advanced planning data and contingency plans;

g) Interfaces with other networks; and

h) Analyses of changes in technology and/or potential service improvements that may enhance DREN services or reduce costs.

3.1.5.2 Annual DREN Users Conference

The Contractor shall conduct an Annual DREN Networkers Conference to inform DREN site personnel on topics including network performance and status and plans for the coming year. The conference will be open to DREN site points of contact and users located at the DREN SDPs, HPCMP management personnel, Government network management, and security personnel and support Contractors with a role in operation or management of DREN services at the network or SDP level. The Contractor shall perform the following tasks to conduct the Annual Networkers Conference:

a) Obtain the facility;

b) Arrange for all scheduled speakers;

c) Notify DREN site points of contact;

d) Develop a list of attendees and register them upon entrance into the conference;

e) Provide all necessary audio/visual equipment;

f) Provide network access for attendees; and

g) Develop a record of the conference and provide the record to attendees.

The Annual Networkers Conference shall take place at a location approved by the Government.

3.2 IMPLEMENTATION & TRANSITION

The Contractor shall perform the necessary planning and transaction actions to successfully implement and transition the DREN SDPs. During transition, the successful offeror's network must establish and maintain full interoperability with the existing DREN Inter-site Services Contract network.

3.2.1 Planning

The Contractor shall manage the transition of all existing DREN SDPs to the follow-on DREN contract. The transition of existing DREN SDPs will be completed in two phases. The Contractor shall provide, for Government approval, a Comprehensive Implementation & Transition Plan that identifies all task activities and schedule milestones associated with the activities described below for each phase; the general approach along with a timeline and site selections for both initial transition and Phase II shall be submitted by the offeror in reply to this

SOW and a detailed plan will be submitted within 30 days after award (see paragraph 3.2.1.1) . This high level planning shall be in addition to the separate requirement for an SDP Plan that shall be prepared for each SDP (see paragraph 3.3.1.1).

3.2.1.1 Transition Planning (Phase I)

The Contractor shall develop a first version of the Comprehensive Implementation & Transition Plan to achieve full implementation of the DREN services required under Phase I. As part of this plan, the contractor will submit their approach to transition 8 – 10 sites for government approval. The initiation of these SDPs is collectively referred to as Initial Performance Capability (IPC), which will be used by the Government as a milestone to control results prior to issuing further task orders. IPC provides for the installation and testing of this set of SDPs, as well as the initial ramp-up of other capabilities of the DREN services environment. The Contractor shall identify the IPC sites. These sites shall include 1 Network Access Point (NAP), 2 Major Shared Resource Centers, 2 Distributed Centers, and 3 to 5 High Performance Node Sites. This IPC set of task orders, plan(s), and other actions compromise the IPC work package. Native IP multicast will be available during this phase.

After award, the Government will provide to the Contractor, all available engineering, technical data from the existing contract to assist the Contractor in development of the detailed Implementation and Transition Plan which will be due within 30 days. The Comprehensive Implementation & Transition Plan shall include, as a minimum, the elements described in paragraph 3.2.1.3 below.

3.2.1.2 Transition Planning (Phase II)

After successful completion of Phase I, the Government will issue one or more task orders to initiate the remainder of the SDPs that currently comprise the DREN. The initiation of these remaining sites is collectively referred to as Phase II. Phase II provides for the testing of this set of SDPs and any additional DREN service capabilities not completed as part of Phase I.

Upon initiation of Phase II, the Contractor shall update, revise, and complete (as applicable) the Comprehensive Implementation & Transition Plan to account for the work to be performed during Phase II.

3.2.1.3 Content of Comprehensive Implementation & Transition Plan

The Comprehensive Implementation & Transition Plan shall include, at a minimum, information pertaining to the following planning elements:

3.2.1.3.1 Transition

The Contractor's plan shall provide detail for transitioning services from the existing DISC to the follow-on DREN contract. The Contractor shall use a Government-provided inventory of customer locations, facilities, and services as the basis for development of the plan. The Contractor shall ensure that the plan describes all aspects of the transition process, including logistics, emergency procedures, and database and operation support system requirements and uses. The Contractor shall include in the plan requirements for interconnecting the existing network with the new Defense Research Engineering Network to ensure a transparent transition with minimum effects on service quality and availability. The plan shall include plans and procedures for conducting site surveys. The Contractor shall describe the approach for serving as the single point of contact during service transition, and the activities and functions it will perform to coordinate activities with Government personnel and other Contractors as necessary. The Contractor shall also describe an approach for coordinating with site personnel and carriers to resolve service troubles encountered during implementation and site cutover.

3.2.1.3.2 Interoperability

The Contractor's plan shall provide detail for interoperating with the other telecommunications networks and services. The Contractor shall describe an approach for interfaces and interoperability in terms of the full range of applicable communications functions, including addressing plans, access control, network management, signaling, and timing and synchronization. The Contractor shall also specify interfaces and inter-connectivity between the DREN network and other networks, and define its approach for working with the service providers for these other networks. The Government will provide an autonomous system number (ASN), IP address blocks, NSAP address blocks, and domain names that will be used for the DREN community between internal and external networks. The Contractor will be responsible for managing the administration of these items (See Section 3.3.3, Services at SDPs That Perform Gateway Functions).

3.2.1.3.3 Security

The Contractor's plan shall detail the approach for implementing the security requirements detailed in Section 4 of this SOW.

3.2.1.3.4 Implementation Schedule

The Contractor's plan shall provide an implementation schedule that describes the Contractor's schedule for completing the transition/implementation. The Contractor shall develop milestones for all facets of the engineering, implementation, and testing activities required to implement and deploy services to each end-user SDP. The Contractor's implementation schedule shall conform to the priorities established by the Government for cutover of specific end-user SDPs. Schedule data shall be provided using Microsoft Project application software.

3.2.1.3.5 IPC Acceptance Test

The Contractor's plan shall describe the acceptance testing procedure to be used . For IPC Phase 1 a separate collective test plan will be developed by the offeror. As a means of examining the effects and impacts of the simultaneous operation of sets of active SDPs, the Contractor shall perform a Collective Test. The Contractor shall complete a Collective Test upon completion of IPC Phase I transition (which shall not be separately priced). The Contractor shall utilize only Contractor-provided resources; no Government CPE shall be utilized. Such tests shall, as a minimum, address the following test considerations that are applicable to sets of SDPs:

a) Demonstration of the operation of the Digital Data Transfer Services to comply with Section 3;

b) Demonstration of successful completion of routine service configurations for SDPs;

c) PVC/SVC setup and tear-down;

d) ATM Quality of Service (QoS) class changes;

e) ATM PVC traffic contract parameter changes; and

f) Additional criteria to verify the services required by SDPs, as set forth in the Contractor's proposal incorporated as part of the contract upon award.

The Contractor shall execute the Collective Test under the following conditions:

a) As a part of the IPC Work Package; and

b) When ordered by the Government;

c) The Government reserves the right to witness the Collective SDP Test.

Upon completion of the IPC Phase I Test, the Contractor shall submit a IPC Phase I Test Report documenting all results of the execution of the test(s).

3.2.1.3.6 Cutover

The Contractor shall describe a generic, overall approach for cutover of services at all SDPs. The approach at Gateway SDPs may need to be different than for other SDPs; the plan should identify the differences if any.

3.2.1.3.7 Customer Notification

The Contractor shall identify its approach for notifying site communications personnel of pending service cutovers and of pending Contractor-conducted testing 30 calendar days in advance of the date cutover and/or testing activities will begin. The Contractor shall describe its approach for notifying site communications personnel of procedures for using services during initial cutover, and procedures for using new services as they are deployed over the life of the contract. The Contractor shall also describe its approach for supporting site communications personnel in the resolution of end user troubles during the transition period.

3.2.1.3.8 SDP Site Surveys

Upon approval by the Government, the Contractor shall conduct a site survey at each SDP. In the event that a site survey is required, the Contractor shall contact the site POC at least 15 days prior to the survey.

3.2.2 Implementation & Transaction Actions

3.2.2.1 Phase I Actions

Upon order of the Government, the contractor shall execute the approved Comprehensive Implementation & Transition Plan that governs the actions associated with the installation of the Phase I set of SDPs (the IPC Work Package).

The Government may delay the start of the Collective SDP Test, at no further cost to the Government, but such delay may not exceed 10 workdays.

Upon completion of the activities described above, the Contractor shall prepare and submit for Government approval an IPC Work Package Acceptance Report. This report shall document the full completion of the IPC Work Package and as a minimum shall include a copy of each of the acceptance reports of the separate SDPs, the Collective SDP Test, and other Government-approved tests. At the completion of an acceptable IPC Work Package and approval of IPC Acceptance Test Report, first payments for services will commence.

3.2.2.2 Phase II Actions

Following completion of Phase I implementation, and upon order of the Government, the Contractor shall execute the revised and approved Comprehensive Implementation & Transition Plan that governs the actions associated with the installation of the Phase II set of SDPs. The Acceptance Testing Sub-plan incorporated into the SDP Plan for each SDP shall govern acceptance of the SDPs during this phase.

3.3 STEADY-STATE NETWORKING ACTIONS

3.3.1 Install, Modify, Terminate, and Restore SDPs

The Contractor shall install, modify, terminate, and restore SDPs in accordance with the terms of the applicable Task Order and the SOW. The contractor shall be responsible for obtaining, provisioning and maintaining all equipment and software for each SDP.

3.3.1.1 SDP Plans

The Contractor shall provide an SDP Plan for Government approval for each SDP installation and modification action. With respect to plans for modification actions, the Contractor shall use the content of the original SDP Plan (which was used to install specific SDP) as the baseline to develop the plan for modification. In the event that a site survey is required to complete the plans, the Contractor shall contact the Government identified Site POC at least 15

calendar days prior to the survey to schedule the visit. An example SDP Plan and Site Survey from the previous network is provided as reference.

Each SDP Plan shall, as a minimum, include the following elements described below.

3.3.1.1.1 Site Alteration Sub-Plan

The Contractor, if required, shall prepare a Site Alteration Subplan that shall include the following as applicable:

a) Transmission media construction such as cabling, repeaters, and conduits;

b) Building modifications, if any, necessary to install equipment and run cables;

c) Power, grounding, heating, ventilating, and air-conditioning (HVAC), plumbing, cable, and signal wiring connections;

d) Storage space requirements;

e) Staging area requirements;

f) An analysis of the impact that this action may have on active SDPs at this site and at other sites, including identification of any actions needed to prevent negative impact

g) Associated schedule for accomplishment of the sub-plan, expressed in terms of "actual date of order" and

h) Firm-fixed price, including supporting cost data (i.e., direct costs), for successfully completing the Site Alteration Sub-plan. The Contractor shall be responsible for all costs resulting from inadequacies or omissions in the Site Alteration Sub-plan. The proposed price for the Site Alteration Sub-plan shall be subject to negotiation.

3.3.1.1.2 Installation/ Modification Sub-Plan

The Contractor shall prepare an Installation/Modification Sub-plan that shall, as a minimum, include the following:

a) Identification of planned space, power, grounding, HVAC, plumbing, floor loading, modem and cabling - including use of GFE cabling if available;

b) Storage space requirements;

c) Staging area requirements;

d) Analysis of the impact that this action may have on active SDPs at this site and at other sites, including identification of any actions needed to prevent negative impact; and

e) Associated schedule for accomplishment of the sub-plan, expressed in terms of "number of days after order."

f) Floor plan layout of equipment location, showing rack(s) configuration;

3.3.1.1.3 Acceptance Testing Sub-Plan

The Contractor shall prepare an Acceptance Testing Sub-plan for each SDP in accordance with the requirements of Section 3.3 and shall, as a minimum, include the following:

a) Test procedures, criteria, and supporting tools as described in the Contractor's Proposal; and

b) Associated schedule for accomplishment of the sub-plan, expressed in terms of "number of days after order."

c) A complete listing (in table form) of all requirements from the RFP (i.e. from the SOW and from other portions of the RFP if applicable) that apply to the specific SDP to be tested, including cross-references from each requirement into the applicable test(s) of the Acceptance Testing Sub-Plan;

3.3.1.1.4 SDP Termination/Restoration Sub-Plan

The Contractor shall prepare an SDP Termination/Restoration Sub-plan that, as a minimum, shall include the following:

a) Equipment to be removed upon SDP termination;

b) An analysis of the impact that terminating service to this SDP may have on the remaining active SDPs at this site and at other sites, including identification of any actions needed to prevent negative impact; and

c) Associated schedule for accomplishment of the sub-plan, expressed in terms of "number of days after order."

3.3.1.1.5 Instruction Sub-Plan

The Contractor shall prepare an Instruction Sub-plan that shall provide:

a) The types and amounts of instructional services that the Contractor will provide to the Government in accordance with their Technical Proposal (incorporated as part of the contract upon award) as part of their overall service; and

b) Recommended schedule for accomplishment of the instruction.

3.3.1.2 Alteration, Installation, and Modification

Upon Government approval of the SDP Plan submitted, the Contractor shall:

a) If ordered, execute the government requested Site Alteration Sub-plan; and

b) If ordered, execute the SDP Installation/Modification Sub-plan.

Upon completion of the SDP Plan execution, the Contractor shall submit "as built" site drawings and diagrams.

3.3.1.3 Acceptance Procedures

Upon completion of the SDP Installation/Modification Sub-plan, the Contractor shall execute the acceptance tests from the approved SDP Acceptance Testing Sub-plan.

The Government reserves the following rights:

a) To witness the SDP Acceptance Test;

b) To delay the start of the SDP Acceptance Test, at no additional cost to the Government, but such delay will not exceed two (2) workdays; and

c) To require the Contractor to rerun all or any portions of the SDP Acceptance Test in the event that the SDP fails to satisfy any of the test criteria at no additional cost to the Government;

Upon completion of the SDP Acceptance Test, the Contractor shall submit an SDP Acceptance Test Report, documenting all results for each execution of the Acceptance Test Sub-plan. Once accepted, DREN users shall consider an SDP “active” for functional use until such time that the SDP is modified or terminated.

3.3.1.4 Termination/Restoration

Upon request of the Government, the Contractor shall execute the most recently provided SDP Termination/Restoration Sub-plan as set forth in the most recently approved SDP Plan for the SDP. Upon completion, the Contractor shall submit "as built" site drawings and diagrams.

In the event that a site survey is required to complete the planning, the Contractor shall contact the Government-identified site POC at least 30 calendar days prior to the survey to schedule the visit.

3.3.2 Disaster Recovery and Contingency

The Contractor shall exert "best effort" (best industry practices) to provide continuity of services in the event of disasters, including fires, earthquakes, hurricanes, and flooding. Disasters also include human-related events, such as fraud, vandalism, arson, work stoppages, strikes, civil disturbances, armed conflict, and sabotage. The Contractor shall also protect the transmission services in accordance with the security requirements of this SOW. In the event of a disaster, the Contractor shall implement the Computer/System Emergency Response Plan as described in Section 4.3.8, Continuity of Operations.

3.3.3 Services at SDPs That Perform Gateway Functions

The DREN will use a Government-owned and registered ASN for purposes of identifying itself in peering relationships with other networks. The Contractor shall negotiate related peering relationships at NAPs and other private exchange points, and if necessary shall notify all existing

peering partners in the event that DREN's ASN changes. The Contractor shall negotiate on behalf of the Government for any charges (e.g., co-location charges) levied at network exchange points; the Government shall be responsible for paying such charges. The Contractor will be expected to provide transit to any Tier 1 Internet Service Provider that is not peering with DREN. The Contractor shall be able to isolate DREN from any network or exchange, or make changes to associated Access Control Lists, upon direction from the Government (See Section 4.1.1).

3.4 DIGITAL DATA TRANSFER SERVICES

The Contractor shall provide digital data transfer services in accordance with the following.

3.4.1 SDP Characteristics

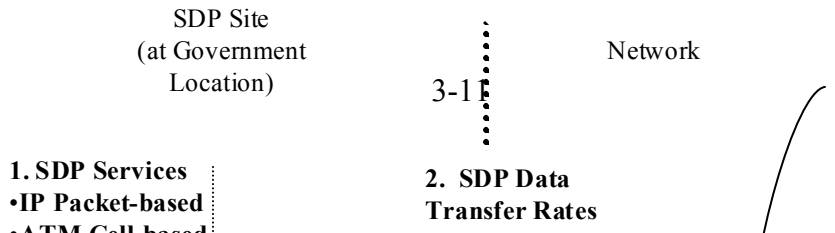
The Contractor shall provide continuous, uninterrupted concurrent multi-protocol digital data transfer services between active SDPs. SDPs shall be defined in terms of the following elements:

1. SDP Services provide the interface between the SDP and the user CPE, based on interface standards and data transfer rate.

2. SDP sustained and peak data transfer rates, which specify the available data transfer rates available for all Government traffic in aggregate generated at an SDP, through the equipped services at that SDP regardless of protocol or format, for transmission through the network to other SDPs.

These SDP elements are illustrated in Figure 3-1.

Figure 3-1
SDP Characteristics



3.4.1.1 SDP Services

The Contractor shall provide continuous, uninterrupted, concurrent multi-protocol digital data transfer services between and among active SDPs using the following SDP Service types:

a) ***Service Type A, IP Packet-based*** — Deployed to support IP over ATM or IP delivered via Fast Ethernet, Gigabit Ethernet (including jumbo frame sizes of at least 9000 bytes), or related packet interfaces;

b) ***Service Type B, ATM Cell-based*** —ATM native data with ATM cells delivered to the SDP via standard electrical and/or optical interfaces, for transmission over established virtual circuits. The provider will allow layer 2 signaling across the WAN using all mainstream ATM QOS parameters e.g. UBR, VBR, and CBR. Standard ATM services by the provider will include PVPs, PVCs, SVCs, SPVCs, or other industry standard ATM VCs with UBR, VBR, and CBR QOS.

c) ***Service Type C, Lightwave*** — Although not a service, Lightwave is a method to deliver IP services or possibly, ATM cell-based services.

IP traffic transmitted into a network SDP through a SDP Service Type A will be routed directly by the network to other SDPs supporting IP packets.

ATM cells transmitted into a network SDP through a SDP Service Type B will be switched to the appropriate virtual circuits to other SDPs supporting ATM. The network shall be capable of supporting ATM virtual circuits to carry user data to this internetworking capability.

Type C at an SDP shall deliver IP or ATM cell traffic to the network for routing to other SDPs supporting other Service Types (A, B, or C). The framing formats and interface connectivity shall be based on emerging standards, and shall support technologies not included in Service Types A or B.

All SDPs shall be capable of supporting any combination of these services; the Contractor shall not require the Government to install separate SDPs to support specific interfaces or types of

traffic; for example, the Contractor shall not require separate SDPs at an SDP site for ATM and IP traffic.

Each SDP Service will be defined in terms of an industry-standard data communications interface, which shall include the protocol and maximum SDP/CPE data transfer speed. The interfaces for Types A, B, and C SDP services are provided in Table 3-1.

All interfaces supporting SDP Services shall be either based on appropriate twisted pair or fiber interface standards. The Contractor shall not require equipment supporting SDP services requiring coaxial cable interfaces. All SONET-based interfaces for all interface types shall be based on Concatenated SONET interface standards.

TABLE 3-1
SDP Service Classifications

SDP Service Category	Interface Standard	Physical Interfaces
Service Type A, IP Packet-based	Fast Ethernet	100BaseT
	Fast Ethernet	100BaseF
	Gigabit Ethernet	1000Base-TX
	Gigabit Ethernet	1000Base-SX
	Gigabit Ethernet	1000BaseLX
	10-Gigabit Ethernet	10GBaseSX
	10-Gigabit Ethernet	10GBaseLX
	ATM *	OC-3c Single Mode
	ATM *	OC-3c Multi-Mode
	ATM *	OC-12c Single Mode
	ATM *	OC-12c Multi-Mode
Service Type B, ATM Cell-based	ATM	OC-3c Single Mode
	ATM	OC-3c Multi-Mode
	ATM	OC-12c Single Mode
	ATM	OC-12c Multi-Mode
	To be defined	To be defined
Service Type C, Lightwave	To be defined	To be defined

3.4.1.2 SDP Data Transfer Rates

Each SDP shall have the capability to support two-way full duplex aggregate sustained and peak data transfer rates to the rest of the network for all data traffic managed by that SDP through all interfaces. The sustained and peak data rates for an SDP will be specified by the Government from seven sustained/peak data rate pairs listed in Table 3-2. These rates apply to all user traffic at an SDP, regardless of protocol or SDP Service at the originating or terminating SDP.

TABLE 3-2
SDP Sustained and Peak Rate Combinations
(All data rates in Mbps)

SDP Peak Rates	36.0	124.0	497.6	995.2	1990.4	7952.0	31808.0

* *Example: Customer Premise Router with an AIP interface*

(80% of line Speed)							
SDP Sustained Rates (50% of line speed)	22.5	77.5	311.0	622.0	1244.0	4970.0	19880.0

The sustained and peak rates shall apply to all user data transmitted to an SDP through the equipped SDP Services (Types A, B and C), excluding cell and/or protocol overhead needed for routing the user data to the destination user device at the destination SDP.

The Contractor shall engineer and install access capacity at each SDP to support the sustained and peak data rates specified by the Government for that SDP at the time the SDP is ordered. The Contractor shall expand access capacity at an SDP should subsequent modifications to the sustained and peak data rates for services exceed the available access capacity at that SDP.

The Contractor shall provide the capability to support IP version 6 (IPv6) through all services delivered through all SDPs when IPv6 becomes available through commercial service offerings. The contractor shall support the Government in transition from IPv4 to IPv6.

3.4.2 SDP Functional Requirements

Each SDP shall operate independently of other SDPs but in a manner that complies with requirements for interoperability.

The Contractor's service shall transfer data between and among simultaneously connected SDPs in such a way that:

a) The ability to provide concurrent digital data transfer services to other active SDPs shall not be negatively impacted;

b) Any inter-networking functions that implement requirements shall be maintained;

c) The ability to utilize the SDP capabilities that implement requirements shall be maintained; and testing of this capability at an SDP shall not negatively impact the services provided via any other SDP;

d) The ability to transfer data between SDPs shall be possible at the subscribed access rates mutually available between the two SDPs;

e) SDP Services shall be able to transfer data limited by the interface standard for the Service interface and the sustained and peak data transfer rates for SDP

f) The Contractor shall design SDPs such that individual SDP Services can be added or eliminated without impacting other existing CPE interfaces, regardless of Service type.

The Contractor shall manage active SDPs in a manner that permits the Government to utilize the SDP performance capabilities on demand.

3.4.2.1 SDP and VC Availability Requirements

Each active SDP shall experience no more than 30 minutes of outage per month. Billing credits for such outages shall be provided according to the schedule specified in Table 3-3. The contractor shall also satisfy PVC and SVC availability requirements specified in Table 3-4. The definitions used for determining SDP, PVC, and SVC availability are provided below.

3.4.2.1.1 SDP and VC Availability Definitions

a) An ***"Outage"*** is declared and the specific SDP service is considered "unavailable" if that SDP service fails to deliver service in accordance with the terms of this contract;

b) ***"SDP Availability"*** is calculated in minutes that an SDP provides service to Government customers through all equipped SDP Services in accordance with the terms of this contract;

c) ***"PVC Availability"*** is calculated as the percent of time that a PVC provides service to its customers in accordance with the terms of this contract.

d) ***"SVC Availability"*** is calculated as the percent of connection set up requests completed in accordance with the terms of this contract.

3.4.2.1.2 Determination of SDP Service Availability

All periods of SDP degradation shall be considered periods that the SDP and/or its equipped services are not available. All periods of time that an SDP service is not available and is not otherwise excluded shall be included as outage time in the following calculations. The following periods of time shall not be included in the determination of system outage:

a) Time during which planned, scheduled activities that the Government has approved, such as preventive maintenance, disrupt service;

b) Time during which Government-attributable causes, such as when loss of Government-provided power disrupt service; and/or

c) Time during which delays on the part of the Government, such as providing access to site facilities, disrupt service.

3.4.2.1.3 Billing Credits for SDP Outages

Billing (outage) credits are provided when an the SDP does not meet the SDP service availaibility requirements as specified in the paragraph 3.4.2.1. Such billing credits will be reflected on the monthly invoice. Billing credits will be given for SDP outages according to the schedule in Table 3-3, and billing credit calculations will commence after 30 cumulative minutes of SDP outage during any calendar month. These credits are not mitigated by the time intervals specified in Table 3-9 Required Response and Repair Times for trouble resolution as required in paragraph 3.7.2.2.1.

TABLE 3-3
Determination of Outage Credits for SDP Availability

Length of Interruption	Credit Per Interruption*
31 minutes up to, but not including, 2 hours	5.0 %
2 hours up to, but not including, 4 hours	10.0 %
4 hours up to, but not including, 6 hours	15.0 %
6 hours up to, but not including, 8 hours	20.0 %
8 hours up to, but not including, 10 hours	25.0 %
2 hours up to, but not including, 12 hours	30.0 %
2 hours up to, but not including, 14 hours	35.0 %
2 hours up to, but not including, 16 hours	40.0 %
2 hours up to, but not including, 18 hours	45.0 %
Over 18 + hours	50.0 %
* % Credit applies to SDP monthly recurring charges	

3.4.2.1.4 Calculation of PVC and SVC Availability

For PVCs and SVCs, availability measures are calculated as shown in Table 3-4.

TABLE 3-4
Determination of SDPs and VCs Availability for DREN Services

QoS Parameter	Calculation	DREN Requirements
(Per) PVC Availability[1,]	$\{ 1 - \frac{\text{(PVC outage in Hours during a Month)}}{\text{Hours in the Month}} \} \times 100$	≥99.5%
(Per) SVC Availability[1,]	{ 1 – Number of setup requests completed in busiest hour/ Number of Call setups requested in the same busiest hour) } x 100	≥99.5%

Note 1 – Applies to SDPs able to establish VCs.

3.4.2.2 PVC Failsafe

When a PVC experiences severe degradation or hard failure, within 10 ms of the occurrence of the degradation or failure condition, the system will invoke SPVC call set up to establish a new PVC.

3.4.2.3 IP Performance/Packet Loss

Performance characteristics of the network (minimum loss, errors, latency, etc) must be sufficient to sustain a single TCP/IP flow at or above the SDP sustained data transfer rate. This applies to all SDP service types (A, B, C). This must be demonstrated at IPC and at other times at the government's request between any two SDPs to verify continued compliance with this performance metric. The demonstration/test must show that a TCP/IP flow can be sustained at or

above the SDP sustained data transfer rate between 2 computers connected to separate SDPs. The test must use a standards compliant, off-the-shelf TCP/IP implementation in the computer at each endpoint. This test must be at least 10 minutes in duration. The IPC demonstration must include but is not limited to a wide-area (preferably coast-to-coast) test between two OC-12 sites. This IPC demonstration must include tests where the computers are connected via Gigabit-Ethernet interfaces (verification of Type A service) and where the computers are connected via the Type B service (verification of end-to-end ATM performance). It is understood that the network traffic at the participating SDPs will need to be at or near idle during this test. For a more detailed discussion of this requirement, see Attachment D.

The loss of IP packets submitted to the network shall not exceed 0.1% at any time (where the offered load to the network does not exceed the peak data transfer rate, nor exceeds the sustained data transfer rate for more than tens of minutes). Any loss greater than this, or an inability to achieve the TCP/IP performance levels as described above, will be considered an "outage". The contractor shall measure packet loss and report results daily.

3.4.3 Network-Related SDP Performance Requirements

The Contractor shall provide the following performance for the ATM PVC/SVC service parameters defined in Table 3-5.

TABLE 3-5
ATM VC Service Requirements

Parameter	Definition	rt-VBR	nrt-VBR	UBR	CBR
CTD	Cell Transfer Delay (critical for real-time interactive services for voice, video, etc.)	Distance Dependent[1]	Unspecified	Unspecified	Distance Dependent[1]
CDV	Cell Delay Variation (critical for real time interactive services for voice, video, etc.)	Distance Dependent[2]	Unspecified	Unspecified	Distance Dependent[2]
CLR (CLP*- = 0+1)	Cell Loss Ratio with no distinction between Cell Loss Priority of 0 or 1	10^{-7}	10^{-5}	Unspecified	10^{-7}
CLR (CLP* -= 0)	Cell Loss Ratio with CLP of 0	N/A	Unspecified	Unspecified	N/A
CER	Cell Error Rate	$4 * 10^{-6}$	$4 * 10^{-6}$	$4 * 10^{-6}$	$4 * 10^{-6}$
CMR	Cell Misinsertion Rate	1 per day	1 per day	1 per day	1 per day

Note 1: The CTD should be dependent upon the distance between the communicating SDPs.

Note 2: The CDV should be dependent upon distance between the communicating SDPs and proportional to CTD with the maximum CDV less than tolerable for compressed voice or video communication.

The Contractor shall satisfy the performance objectives for IP services specified in their technical proposal and incorporated as part of the contract.

Maximum roundtrip time (latency) for traffic over similar IP, ATM, or POS services deployed at two SDPs shall be governed by distance between those SDPs according to the following rule:

$$\text{Roundtrip Time (in milliseconds)} = 20 + [.02 * \text{Inter-SDP distance in kilometers}]$$

Inter-SDP distance shall be established as line-of-sight. For example, roundtrip delay over an ATM PVC/SVC connecting two DREN SDPs 650 kilometers apart must not exceed 33 milliseconds. As a second example, roundtrip delay for IP traffic entering the network between two SDPs 3000 kilometers apart must not exceed 80 milliseconds. Traffic between all shall be governed by this requirement.

After acceptance, delay measurements shall be performed by the Contractor using Internet Control and Management Protocol (ICMP) Ping messages generated and measured at all networked SDPs once per minute, 24 hours per day year round and report results daily.

3.4.4 Contractor Verification of Services

3.4.4.1 Individual SDP Test

Upon installation or when ordered by the Government, the Contractor shall execute the SDP Acceptance Testing Sub-plan contained in the most recently completed SDP Plan.

Upon completion of the requested test the Contractor shall submit an SDP Test Report documenting all results of the execution of the test(s).

3.4.4.2 Collective SDP Test

As a means of examining the effects and impacts of the simultaneous operation of sets of active SDPs, the Contractor shall perform a Collective SDP Test (i.e., tests of sets of SDPs). The Contractor shall complete a Collective SDP Test upon completion of IPC as part of transition (which shall not be separately priced). After IPC, the Contractor shall perform additional Collective SDP Tests as ordered by the Government (which shall be separately priced). The Contractor shall utilize only Contractor-provided resources; no Government CPE shall be utilized. Such tests shall, as a minimum, address the following test considerations that are applicable to sets of SDPs:

a) Demonstration of the operation of the Digital Data Transfer Services to comply with Section 3;

b) Demonstration of successful completion of routine service configurations for SDPs;

c) PVC/SVC setup and tear-down;

d) ATM Quality of Service (QoS) class changes;

e) ATM PVC traffic contract parameter changes; and

f) Additional criteria to verify the services required by SDPs, as set forth in the Contractor's proposal incorporated as part of the contract upon award.

The Contractor shall execute the Collective SDP Tests under the following conditions:

g) As a part of the IPC Work Package; and

h) When ordered by the Government;

i) The Government reserves the right to witness the Collective SDP Test.

Upon completion of the Collective SDP Test, the Contractor shall submit a Collective SDP Test Report documenting all results of the execution of the test(s).

3.4.4.3 Government Verification of Services

The Government shall have the right to access SDP equipment for independent testing and evaluation activities with advance notice to the contractor.

3.4.5 Local Connectivity from SDP Sites to Secondary Sites

The Government shall have the option to require the Contractor to provide and manage local connectivity between a SDP at a SDP site and a secondary site. This connectivity shall be provided from the interface for an SDP service through a local transport facility to be provided by a local carrier, to a demarcation point at the secondary DREN site. The Government and the Contractor shall determine a mutually acceptable approach regarding: ordering, installation, and management of LEC transport services; providing equipment at the SDP and secondary sites to support this connectivity; and management of inside wiring. The Government shall be responsible for link utilization and performance of Government-provided equipment and cabling at the SDP and secondary sites. The Contractor's responsibility for this connectivity shall include management and routine maintenance; trouble isolation between Government, Contractor, and LEC facilities; and restoration of the link. The contractor's responsibility for SDP services will not extend beyond the SDP at the SDP site.

The Contractor shall provide the Government with a proposal for local connectivity at the request of the Government, which shall include but not be limited to: all engineering services, materials (not including equipment), the LEC services to be provided for the connectivity, and the non-recurring and monthly recurring charges for the connectivity service. The costs for LEC services, if provided by the Contractor, shall be included in the monthly recurring charge. The Government shall have the right to accept or refuse the Contractor's proposal. If accepted, the Contractor shall update the SDP Plan and related sub-plans for the SDP at which the local connectivity service is to be provided.

This connectivity may be requested by the Government on an SDP-by-SDP basis. The Government is not obligated to request local connectivity at any SDP. Currently, the Government is using local connectivity to connect several secondary sites to a DREN SDP in the Norfolk, VA area.

3.5 EVOLUTION OF EXISTING SERVICES

An objective of this contract is to acquire state-of-the-art digital data transfer services that are recognized to be constantly evolving. The Contractor shall initiate/support technology insertion efforts and/or system upgrades to maintain state-of-the-art, commercially available services and compatibility with evolving technologies and standards.

Standards applicable to services provided under this contract are defined by standards-governing organizations (stated in order of decreasing precedence) such as the Internet

Architecture Board (IAB), the Internet Engineering Task Force (IETF), the ATM Forum, Bellcore, the American National Standards Institute (ANSI), and the International Telecommunication Union (ITU). The Contractor shall assist the Government in ensuring that services (including testing and analysis) provided under this contract remain compatible with current state-of-the-art versions of the applicable standards.

3.5.1 Technology Insertion

Upon commercial availability of new enhancements that can be substituted for, or added to, services identified in the Contractor's Proposal, the Contractor shall submit technology insertion proposals both independently and in response to Government requests.

These item(s) may be accepted at the option of the Government. The Technology Insertion Proposal shall contain, as a minimum, the following information:

a) A description, in detail, of the difference between the existing contract items and/or services and those proposed, and a specific analysis of the comparative advantages and disadvantages of each;

b) A statement as to how the changes will affect performance, costs, etc., if adopted;

c) An evaluation of the effects the change would have on Life-Cycle-Costs such as existing services, site modification, energy, etc.; and

d) An analysis of a timeframe in which the change should be instituted to obtain maximum benefit to the Government for the remainder of the contract.

The decision as to the acceptability of a Technology Insertion Proposal shall be at the sole and exclusive discretion of the Contracting Officer and not subject to the Disputes Clause of this contract.

3.5.2 Upgrades

The Contractor shall offer the Government any upgrades, generic or version, etc. to SDPs that will enhance Government's use of the DREN. Upgrades and enhancements that are provided to the Contractor routinely by equipment and software suppliers, as a part of the Contractor's equipment and software maintenance contracts, shall be provided to the Government at no additional cost. For upgrades that constitute new technology insertions, the contractor shall submit proposals which include a firm price quote, implementation plan, and supporting cost/benefit analyses. Upon approval of the proposal by the Government, the Contractor shall implement and follow acceptance procedures described in the implementation plan. The decision as to the acceptability of a proposal shall be at the sole and exclusive discretion of the Contracting Officer and not subject to the Disputes Clause of this contract.

3.5.3 Government versus Contractor Initiated Proposals

3.5.3.1 Government Initiated

At the Government's request, the Contractor shall prepare a Technology Insertion or System Upgrade Proposal.

3.5.3.2 Contractor Initiated

The Contractor may submit unsolicited Technology Insertion proposals or System Upgrade proposals.

For requirements identified using the term "when commercially available" which are not commercially available at contract award, the Contractor shall prepare Technology Insertion Proposals to implement service enhancements to meet those requirements.

3.6 NETWORK MANAGEMENT

The Contractor shall manage the DREN network to ensure the required services are operational and delivered in accordance with the requirements. Network management consists of four functions: Network Supervision and Maintenance, Fault Management, Performance Management, and Configuration Management (security management is addressed in Section 4.0, Security). Requirements for each of these Network Management functions are defined below.

3.6.1 Network Supervision and Maintenance

The Contractor shall operate and maintain a network operations center 24 hours per day, seven days per week (7 x 24). The network management interface should employ Simple Network Management Protocol (SNMP) for accessing the network information.

The Contractor shall enable the Government to monitor real-time DREN network performance and status using a client version of the contractors own network management system. This information shall be sufficient to enable HPCMP personnel to track problems at DREN SDPs and evaluate performance trends.

In addition, the Contractor shall allow the Government SNMP access to devices within the ASN on a real-time basis. The interoperability between the Contractor and Government network management systems shall allow the Government to monitor DREN associated assets with the specific purpose of comparing various performance parameters of the VPN being delivered to the Government customers.

3.6.2 Fault Management

Fault Management includes the set of activities required for detection, isolation, and correction of service-affecting faults. Fault Management of the DREN shall support the operation and maintenance of DREN resources, and ensure the operation of each service and feature to meet specified requirements. It shall include: detecting failures, maintaining error logs, determining the nature, severity, and the specific cause of the failure; exercising control; and

directing maintenance action, as necessary. The Contractor shall also support cooperative diagnostic testing with the Government to isolate interface problems. Fault Management also includes the following activities at the network and CPE Interface/SDP.

3.6.2.1 Fault Management at Network Level

The Contractor shall monitor network alarms, detect network failures, determine nature and severity of the problem, isolate the fault, and take corrective actions to resolve the problem. The Contractor shall maintain alarm logs and a record of corrective actions taken in a database format that will allow the Government to easily analyze alarm occurrence and correction history.

3.6.2.2 Problem and Fault Isolation – Type A IP Packet-based SDP Services

The Contractor shall provide unambiguous analysis of service failures at SDPs using packet-based interfaces (including SDPs that perform gateway functions) through fault detection and isolation capabilities, and enable service restoration at the SDP.

These capabilities shall, as a minimum, identify the failure location responsibility (either in the Contractor's equipment or in the directly attached CPE) and isolate the problem, when it is in the Contractor's equipment to the physical layer, link layer, network layer, or upper protocol (e.g., BGP) layers of the IP services.

Diagnostic capabilities shall include, as a minimum:

a) Demonstrating end-system (directly attached CPE) reachability;

b) Reporting end-system (directly attached CPE) reachability failures;

c) Detecting and resolving physical layer and physical media failures;

d) Detecting and resolving media access protocol failures;

e) Detecting and resolving address errors and configuration errors at the link layer network layer, and transport layer. These include medium access control addresses, network addresses, application port identifications, defective or mis-configured routing tables, and defective or mis-configured routing policies;

f) Demonstrating conformance to established IP routing policy;

g) Demonstrating interoperability with all SDPs that are required to support IPv4 (native and tunneling of Ipv6 packets); and

h) Demonstrating interoperability with all SDPs that are required to support IPv6 (native and tunneling of IPv4 packets).

3.6.2.3 Problem and Fault Isolation- Type B ATM Cell-based SDP Services

The Contractor shall provide unambiguous analysis of service failures at SDPs using cell-based interfaces (including SDPs that perform gateway functions) through in-band and out-of-band fault detection and isolation capabilities, and enable service restoration at the SDP. SDPs

shall support the latest ATM forum standards (UNI 3.1 and UNI 4.0), and F1, F2, F3, F4, and F5 Operation, Administration, and Management (OAM) cells for fault detection, isolation, reporting, and other network management functions.

These capabilities shall, as a minimum, identify the failure location responsibility (either in the Contractor's equipment or in the directly attached CPE), and isolate the problem, when it is in the Contractor's equipment, to the physical layer, ATM layer, ATM adaptation layer, or upper protocol layers of the ATM services.

Diagnostic capabilities shall include, as a minimum:

a) ATM layer SDP-SDP Virtual Path Connection (VPC) and VPC /Virtual Channel Connection (VCC) connectivity;

b) ATM endpoint continuity check OAM cell usage;

c) VPC and selected VCC Alarm Indication Signal handling;

d) VPC and selected VCC Remote Defect Indication (RDI) handling;

e) Physical segment loopback testing;

f) End-to-end loopback testing;

g) ATM layer address errors and configuration errors detection and resolution. These include address translations, defective or mis-configured address translation tables, and defective or mis-configured route selection policies;

h) Demonstrating conformance to established ATM route selection policy;

i) Demonstrating interoperability with all other SDPs that are required to support ATM cell-based services; and

j) Demonstrating interoperability with all other SDPs that are required to support IP packet-based services.

3.6.2.4 Problem and Fault Isolation- Type C Lightwave SDP Services

The Contractor shall provide unambiguous analysis of service failures at the lightwave SDPs through fault detection and isolation capabilities, and enable service restoration at the lightwave SDPs.

These capabilities shall, as a minimum, identify the failure location responsibility (either in the Contractor's equipment or in the directly attached CPE) and isolate the problem, when it is in the Contractor's equipment, to the physical layer, network layer, or upper protocol (e.g., Border Gateway Protocol) layers as applicable.

3.6.2.5 Problem and Fault Isolation – SDP Utilized as Gateways

In addition to the requirements of Sections 3.6.2.2, 3.6.2.3, and 3.6.2.4, at SDPs that also perform gateway functions, the Contractor shall monitor problems with other networks interfaced at the NAPs, MAEs, and Gigapops and resolve problems with the network management organizations of the other networks. The Contractor shall also keep log of all the problems and corrective actions taken to resolve the problems at these locations.

3.6.3 Performance Management

Performance Management preserves the quality of network services and develops information that is required to evaluate performance through collection and analysis of network data. Performance Management capabilities shall include, as a minimum: gathering performance data, identifying traffic exceptions and performance problems, and correcting performance problems. Performance Management shall also include a traffic management function to optimize the use of network resources when the network is stressed. In accordance with the requirements of Sections 3.6.3.1 through 3.6.3.3, the Contractor shall provide Performance Management at the SDP level that is compatible with Government end-to-end service level management systems, as stated in Section 3.6.5.

3.6.3.1 Performance Measurement and Validation – TYPE A IP Packet-Based SDP Services

The Contractor shall provide a performance measurement and reporting capability to allow unambiguous analysis of service performance, performance over comparable time intervals, computation of performance trends, and validation of a packet-based service delivery at SDPs (including SDPs that perform gateway functions). This capability shall, as a minimum, be capable of quantifying and reporting the following:

a) Sustained and maximum IP output transfer rate at the SDP; and

b) Sustained and maximum IP input transfer rate at the SDP.

3.6.3.2 Performance Measurement and Validation – Type B ATM Cell-based SDP Services

The Contractor shall provide a performance measurement and reporting capability to allow unambiguous analysis of service performance and validation of cell-based service delivery at SDPs (including SDPs that perform gateway functions).

This capability shall, as a minimum, provide:

a) The ability to monitor, in service, individual VPC and VCC performance. Impairments to be quantified include those resulting from transmission errors, intermittent problems experienced by physical facility impairments, and the combined anomalies affecting all facilities that support end-to-end Virtual Path (VP) or VC connections;

b) The ability to monitor ATM service performance impairments due to VP and VC soft failures, intermittent troubles due to protocol errors and protocol implementation incompatibilities, software problems at the ATM layer, and temporary actions taken

by ATM switches to alleviate network congestion or to control the usage of shared ATM resources;

c) Support for commercial ATM VPC/VCC performance monitoring schemes, both in-service and out-of-service;

d) Support for standard performance monitoring OAM cell formats and procedures on ATM VPs and VCs. Specific ATM OAM performance functions to be supported include, but are not limited to, forward monitoring, backward reporting, and combined monitoring and reporting functions of: missing or lost cells; bit error patterns; extra or misinserted cells; cell delay and delay variation; and

e) The ability to measure, in service, the ATM layer QoS parameters on individual VPs and VCs, without impairing user traffic. Candidate ATM QoS parameters that shall be measurable include, as a minimum, the Cell-Loss-Ratio (CLR), Cell Transfer Delay (CTD), Cell-Delay-Variation (CDV), Cell Error Rate (CER), and Cell Mis-insertion Rate (CMR). Objectives (consistent with ITU-T Recommendation I.356) for these parameters are shown in Table 3.3.

3.6.3.3 Performance Measurement and Validation – Type C Lightwave SDP Services

The Contractor shall provide a performance measurement and reporting capability to allow unambiguous analysis and system performance validation of service delivery and SDPs using a lightwave CPE interface.

3.6.4 Configuration Management

Configuration Management is the process that preserves the integrity of the network configuration. Configuration Management shall provide Government personnel with access to the Contractor's network management database containing the configuration management data. This capability shall allow Government personnel to monitor the configuration of network components supporting services rendered to the Government. Available configuration information shall include, but is not limited to, the following:

a) Set-up of PVCs, SPVCs, virtual paths and NSAP addressing configurations;

b) IP subnet structure, routing table configurations;

c) Circuit/trunk number;

d) State of the network elements (such as in service, out of service for routine or diagnostic test, disconnected, new, etc.);

e) Inventory of ports and services at each SDP including customer access and network access;

f) Any other equipment installed by the Contractor to provide service such as power, rectifiers, UPS, HVAC, etc.; and

g) Software releases.

Configuration Management data shall include information indicating the date and time of new installations. Information on out-of-service elements shall indicate the date and time of state change and expected return to service. Configuration information of relevance to individual DREN customers shall be available to those customers via the World Wide Web.

The Contractor shall also retain a history of configuration changes and associated service order requests where applicable. The Contractor shall provide configuration information in an electronic format that will enable the Government to review and validate configurations in real time.

3.6.5 Network Management Reporting

Report monitoring for ATM and IP is essential on a real-time basis and on a longer time scale average basis to plan service level objectives, verify service, and troubleshoot problems. The value is not only to confirm that the contracted service is delivered, but also to be able to determine quickly whether some action is required to avert network performance problems, or whether the basic design and service options are appropriate to deliver the expected service. The metrics should include component system availability, performance, and serviceability.

The Contractor shall provide real-time reporting of DREN network management information, via graphical interface to the HPCMP community or other Local Control Center (LCC) as designated by the Government. The reporting utility will provide the ability to generate reports automatically, either periodically as directed by the Government or from the triggering of performance or fault thresholds. If threshold based, the thresholds shall be adjustable with respect to either time or event counts. Reports may cover trouble ticketing and fault management activities, network performance or configuration status, security events or status, and accounting information. The Contractor will work with the Government to establish an acceptable format for generated reports.

At a minimum, the Contractor shall provide the following information pertaining to overall network performance:

a) Individual SDP and SDP Service availability for all SDPs and interfaces as defined in section 3.4.2.1;

b) Service degradation time – the time when there is a severe deterioration in performance of the network;

c) VC Availability – provided in real time and measured as defined in Section 3.4.2.1;

d) Mean Time to Respond - measured as a monthly average of the time from inception of trouble ticket until repair personnel are on site as follows:

   (i) Mean Time to Respond = (Total Time (in Hours) to Respond for All Trouble Tickets That Require On-Site Maintenance)/Total Number of Trouble Tickets That Require On-Site Maintenance;

e) Mean Time to Repair or Restore – measured as a monthly average of the time from inception of trouble ticket until outage is repaired to customer satisfaction as follows:

(i) Mean Time to Restore (Without On-Site Dispatches) = (Total Outage Time (in Hours) for All Trouble Tickets That did not Need On-Site Dispatches)/Total Number of Trouble Tickets That did not Need On-Site Dispatches

(ii) Mean Time to Restore (With On-Site Dispatches) = (Total Outage Time (in Hours) for All Trouble Tickets That Needed On-Site Dispatches)/Total Number of Trouble Tickets That Needed On-Site Dispatches.

3.7 CUSTOMER CARE

The Contractor shall be responsible for providing a Customer Care capability to facilitate DREN customers and HPCMO in:

a) Provisioning and tracking of routine service requests and task orders;

b) Reporting and tracking of DREN problems;

c) Monitoring of Contractor's performance;

d) Accounting management; and

e) Obtaining customer support and instructional services.

The customer care center shall provide toll free access for customers to initiate service requests or report service problems via a help desk. The following sections outline the Contractor's responsibilities pertaining to service provisioning, service and problem management, reporting, accounting management, and customer support services.

3.7.1 Service Provisioning

The Contractor shall be responsible for provisioning and tracking all ordered services. Service provisioning includes install, modify, terminate, and restore SDPs in accordance with the requirements of Section 3.3.1 and configuration of VCs between SDPs. Service shall be provisioned through Service Requests and Task Orders. The Contractor shall coordinate with the Government to ensure all services required in Service Requests and Task Orders are provisioned.

3.7.1.1 Service Requests and Task Orders

The Contractor shall support service requests and tasks orders as delineated below.

3.7.1.1.1 Service Requests

Service Requests (SR) are routine requests for IP configuration changes or for configuration of VCs including activation, change or deactivation of VCs and other activities that are performed as day-to-day operation by the Operations and Maintenance (O&M) staff. The Contractor shall support receiving routine service requests by its Help Desk (Section 3.7.2.1) on a 7 x 24 basis (24 hours a day, 7 days a week, every week).

3.7.1.1.2 Task Orders

The Task Order (TO) includes non-routine requests for activities that are not performed by the O&M staff as a day-to-day operation. The TOs will be initiated by the HPCMP Contracting Officer (CO) to the Contractor. The Contractor shall only process task orders issued by the HPCMP CO or other designated authorized representative.

The Contractor shall provide a TO Request procedure that will enable the HPCMP Contracting Officer to authorize TOs electronically using a software-based TO request system available through a web interface. The CO shall also be able to authorize TOs by regular mail, fax, or other electronic means.

3.7.1.2 Provisioning of Service Requests and Task Orders

The Contractor shall satisfy the requirements associated with routine service requests, task orders, and expedited task orders as delineated below.

3.7.1.2.1 Provisioning of Routine Service Requests

The following delivery intervals depicted in Table 3-6 are required for routine service requests.

TABLE 3-6
Required Routine Delivery Intervals

Service	Standard
PVC Provisioning:	
• New PVC provisioning	3 days
• Change PVC capabilities	3 days
• Delete PVC	5 days
• Move PVC	3 days

The Contractor shall provision service requests on expedited basis upon specific request by the customer representative. Contractor shall also be responsible for ensuring that the services are not oversubscribed.

3.7.1.2.2 Provisioning of Task Orders

Unless otherwise required by a TO, the Contractor shall develop appropriate plans and provision services in accordance with the requirements in Section 3.2.2. The following delivery intervals depicted in Table 3-7 are required for TOs.

TABLE 3-7
Required Provisioning Intervals for Task Orders

Service	Standard
Installation of new services	180 days maximum
Service termination	30 days
Service modifications:	
• Wide area access	180 days
• Local area access	30 days
SDP restoration – fault management	3 days
SDP restoration – clean-up	30 days

The following definitions are provided for clarity:

a) Wide area access — connection from the SDP into the Contractor's wide area network cloud including the LEC "last half mile" infrastructure that the WAN provider has to go through to get to the site.

b) Local area access —the connection from the SDP to the site CPE.

c) SDP restoration — either fault management activities to restore functionality of an active SDP after an outage, or remediation "clean up" activities to the site and network made necessary after an SDP is terminated.

3.7.1.2.3 Expedited Task Orders

The Contractor shall provide service under expedited conditions in accordance with emergency preparedness procedures and policy. These procedures utilize a Provisioning Telecommunications Service Priority order to achieve the described expedite. The Expedited TO may be in the form of electronic mail, fax, telephone call, or verbal request to be followed by a written TO. A written TO will be issued confirming any verbal request. Service provisioning times will be negotiated for each Expedited TO where facilities do not currently exist. The Government requires 72 hours delivery interval for expedited delivery for modifications to DREN services and 30 days expedited delivery for new DREN services. The lack of a written TO does not relieve the Contractor of the responsibility to perform.

3.7.1.3 Service Request and Task Order Tracking

The Contractor shall enter all routine service requests and non-routine TOs in its Customer Service Management system, described in Section 3.6.2.2 and use it to track progress of the request from origination to completion including escalations when they occur. At the minimum, the customer shall maintain record of the following for each routine Service Request/non-routine TO:

a) Service Order request (new, change, move or disconnect);

b) Acknowledgment of request (inquiry);

c) Order modification acknowledgment/completion;

d) Acknowledgment of non-acceptance/acceptance;

e) SDP location;

f) Critical path for activities required for order completion;

g) Customer name, address, telephone number, email address

h) Service/agency name;

i) Account code;

j) Due date;

k) DREN contact name, location, and telephone number;

l) Order status report; and

m) Non-recurring and recurring costs associated with TO.

The provisioning data shall be available to the High Performance Computing Modernization Office (HPCMO) and the customer SDP on a web-based real-time automated basis to allow Government tracking of routine operations or government-initiated task orders. In response to a Government request, the Contractor shall provide complete and timely data on discontinued DREN services for a minimum of 180 calendar days past the date of deactivate or disconnect.

The Contractor shall provide monthly reports that measure the quality of Service Provisioning Performance and includes at a minimum the following information specified in Table 3-8. These reports can be delivered either electronically via email or be made available through a web-based interface.

TABLE 3-8
Quality of Service Reporting Requirements for Customer Care Service Provisioning

Service Provisioning Performance Parameter	Calculation (All Quantities Measured On A Monthly Basis)
Mean time to provision routine Service request (move, add, change or disconnect), PVC or simple SDP parameters (sustained subscription rate, Peak subscription rate)	Cumulative time to respond to all related Service Requests completed during the month/number of Service Requests completed during the month
Mean time to provision SDP service orders by type of service orders	Cumulative time to respond to all related Service Requests completed during the month/number of Service Requests completed during the month

3.7.2 Service and Problem Management

The Contractor shall provide a Service and Problem Management capability to facilitate service ordering and tracking, trouble reporting, and trouble resolution. This capability shall include a help desk, problem management procedures, and a record keeping system.

3.7.2.1 Help Desk

The Contractor shall provide a "Help Desk" function to the Government for customers to report problems related to all aspects of DREN service. The Contractor shall provide a toll free

number to call the Help Desk. Calls to the Help Desk shall be answered 24 hours per day, 7 days per week (7 x 24) every week, by a person authorized to accept and process the report. In addition, the Contractor shall accept Secure Socket Layer (SSL) web-based or digitally signed e-mail service requests and trouble reports and also on the 7 x 24 basis. Calls may come from the HPCMO or the customers served at the SDP sites. Trouble tickets that result in configuration changes to the WAN will only be implemented if initiated or approved by the HPCMO or designated DREN POCs at the sites. The Help Desk shall also acknowledge and track trouble reports submitted by the Contractor's personnel. The Contractor shall create a Service/Trouble Ticket (TT), assign a TT number to the trouble report and shall track and report on each service/trouble report until it is resolved. The Contractor shall address, resolve, and clear all service/trouble reports involving DREN service.

3.7.2.2 Customer Problem Management

The Contractor shall resolve reported troubles and escalate problems in accordance with the following:

3.7.2.2.1 Trouble Resolution

The Contractor shall resolve/correct all reported troubles. The Contractor shall take all necessary actions to resolve troubles, including arrangements for access to the SDPs. The Contractor shall manage trouble resolution for all trouble calls by:

a) Providing real time, on-line status of all open trouble ticket status to HPCMO;

b) Developing a plan for correcting problems that is agreeable to all involved parties; and

c) Correcting the problems in accordance with accepted plans.

The Contractor shall provide trouble resolution capabilities to meet the following requirements delineated in Table 3-9.

TABLE 3-9
Required Response and Repair Times

Category	Time Interval
Time to answer trouble report by human operator	60 seconds
Time to respond to a trouble report	30 minutes
Time to clear trouble report w/o field visit	2 hours
Time to on-site visit by field technician (if required):	
• Key SDP sites designated by HPCMP*	4 hours
• Other sites	5 hours
Time to repair with on-site field visit:	
• Key SDP sites designated by HPCMP*	5 hours
• Other sites	8 hours
• Public peering sites may require on-site technician support to provide shorter response times	

* Key sites are defined as shared resource centers or sites that perform gateway functions.

3.7.2.2.2 Problem Escalation

The Contractor shall provide a problem escalation function within the trouble ticket system to support automated escalation of unresolved problems, including, the generation of an e-mail message to the HPCMO and the SDP/customer when a trouble ticket is escalated. The trouble ticket system shall maintain a list of personnel to be contacted and the contact information, including under what circumstances the next hierarchical person will be notified for certain information including unresolved troubles. A section of the trouble ticket shall contain the name of the last person contacted and the time of contact. The trouble ticket shall also contain the name and title of the next person in line to be called and the projected time for that call.

3.7.2.3 Record Keeping

The Contractor shall implement a Customer Service Management System (customarily known as trouble ticket management system) for record keeping and management of trouble tickets to store and sort trouble records, and maintain an audit trail of maintenance activity and responsibility. Trouble tickets shall be entered and updated by authorized Contractor personnel. Each trouble ticket shall provide:

a) Date and time of reporting;

b) Unique trouble ticket number;

c) Name, telephone number and email address of person reporting the problem;

d) Name, telephone number and email address of person receiving the trouble report;

e) Service/Agency, symptom, priority, component, outage time;

f) Problem SDP site and SDP;

g) Problem description including standard codes for problem classification;

h) Date and time of actions taken to resolve the trouble;

i) Description of corrective actions taken;

j) Description of how service will be verified as working;

k) Date and time of closure of the TT; and

l) Data relating to problem escalation required in Section 3.7.2.2.2.

The data in the trouble ticket shall be available on a web-based real-time automated basis to the HPCMO, and to the customers at the SDP where the trouble is reported. Trouble tickets shall be identified by the unique number for the service/agency, symptom, priority, date, and time. The trouble ticket system shall sort and report trouble tickets by service/agency, symptom, priority, component, outage time, and ticket open and close times, and shall permit analysis of trouble trends and trouble resolution performance. The trouble ticket system shall allow personnel at the HPCMO to match the Contractor's trouble ticket number, including changes or bundling of tickets and escalations, with the trouble ticket number tracked by the HPCMO.

3.7.3 Customer Care Data and Reports

The Contractor shall provide web-based, real-time data, data processing capabilities, and formal, scheduled reports related to DREN trouble handling and resolution. Specifically, the Contractor shall:

a) Maintain historical data on the handling of trouble ticket data for a period of 1 year after resolution of ticket. This data shall be made available in a user-friendly format in both on-line and, when requested, hard copy form to HPCMO;

b) Provide an on-line database of trouble events available to HPCMO management personnel. This database shall list all new trouble calls and all closed trouble tickets for any given day. Reports shall be generated on a daily basis, 7 days per week; and

c) Provide an on-line report generation capability that allows HPCMO management personnel to generate daily, weekly, and monthly summaries of open ticket status, trouble events, and mean time to repair. The Contractor shall enable the Government to generate reports on problem management service quality that includes, but is not limited to, the measurements in Table 3-10.

TABLE 3-10
Quality of Service Reporting Requirements for Customer Care Problem Resolution

Problem Management Performance Parameter	Calculation (All Quantities Measured On A Monthly Basis)
Mean time to respond	Cumulative time to respond to all TTs / Total Number of TTs created
Mean time to repair w/o dispatch	Total outage time for all TTs w/o dispatch / Total number of TTs created
Mean time to visit by field technician — Major sites — Other sites	Total time to visit by a field tech for all TTs w/ dispatch / Total number of TTs requiring dispatch Separately for major and other sites
Mean time to repair with field dispatch — Major sites — Other sites	Total outage time for all TTs with dispatch / Total number of TTs created Separately for major and other sites
Percent of TTs cleared within time intervals specified in Section 3.6.2.2	TTs cleared within designated time limits * 100 / Total number of TTs created Separately for major and other sites
Total number of TTs	Per trouble desk report
Percent TTs requiring field visit	Number TTs requiring dispatch * 100 / Total number TTs created
Percent TTs escalated (by level of escalation) by TT type	Number TTs requiring escalation * 100 / Total number TTs created
Percent Trouble reports answered within designated time interval	Cumulative time to respond to all TTs / Total Number of TTs created Separately for initial response and response by human operator

The Contractor shall provide to the HPCMO the capability to copy all trouble data provided in accordance with this section to hard disk or other media and provide the capability for the HPCMO PM to generate, save, and print reports that are derived from the data.

3.7.4 Accounting Management

Accounting Management consists of the activities associated with collection, aggregation, recording, and distribution of data on DREN quality of service, costs and credits. The Contractor shall collect, aggregate, record, and distribute data to generate/validate billing charges for the services provided and credits for missing quality of service objectives.

The Accounting Management data shall be available to the HPCMP in a user-friendly format with web access.

3.7.5 Customer Support and Instructional Services

The Contractor shall provide support to DREN customers for engineering studies and instruction on DREN services.

3.7.5.1 Instructional Services

The Contractor shall provide instructional services (e.g., formal, informal, self-paced, automated, remotely accessed) to Government-designated personnel (including DREN end users, site operators, and site managers) for the purposes of fully understanding/utilizing the services provided under this Contract.

As a minimum, the instructional services shall address how to:

a) Report DREN-related problems and follow-up on previously reported problems;
b) Utilize the SDP analysis and testing capability;
c) Request SDP routine operational services; and
d) Perform SDP setup for connectivity to the WAN.

If instruction is provided at a Government facility, the Government will provide access to and use of classroom space, equipped with lighting, seating, and writing surfaces for students receiving such training.

3.7.5.2 Technical Support Services

The Government may request through separate task orders technical services to support Government management and operation of the DREN network as a whole or for a specific SDP. The Contractor shall prepare a proposal for performing technical support services in response to a task order statement of work. Labor categories for these efforts are identified in attachment C.

The proposal shall contain sufficient detail to enable the Government to determine the acceptability of the proposal and shall include, as applicable:

a) A brief description of the technical approach which demonstrates the Contractor's understanding of the requirement;

b) A proposed milestone chart or schedule;

c) Proposed labor categories and resumes; and

d) Proposed price (firm-fixed price or time and materials cost).

The Government reserves the right to accept or reject any proposal for technical support services. This decision shall be final and not subject to the "Disputes" clause of this contract. After the Government has reviewed and accepted the Contractor's proposal (negotiations may be required), subject to availability of funds, a task order will be issued.

3.7.5.3 Telecommunications-Related Support

Telecommunications-related technical support services shall include performance of engineering and other telecommunications-related technical activities, which may be needed by the Government as a supplement to the work performed under this contract.

3.7.5.4 Engineering Studies

Engineering Studies technical support services shall include studies related to the present and possible future physical and performance characteristics of Contractor-provided equipment used in the DREN environment, which may be needed by the Government as a supplement to the work performed under this contract. Examples of such studies could include, but are not limited to, system engineering feasibility studies; network studies; technical or technology assessment studies; and quality-related practices studies. These services will be ordered pursuant to Section 3.7.5.2.

3.8 CONTRACT PHASE-OUT

The Contractor shall perform the contract phase-out activities necessary to support the transition to replacement services in the event that the services under this contract are discontinued. All work under SOW Section 3.7 will be initiated through separate task orders. The task orders will define the precise nature of the activity that is required. The contract phase-out subtasks that the Contractor may be required to perform to support transition from DREN to replacement services are described below.

3.8.1 Planning and Engineering Support

The Contractor shall provide phase-out planning and engineering support that includes, but is not limited to, the following activities:

3.8.1.1 Development of Contract Phase-Out Transition Plan

As directed by the task order, the Contractor shall coordinate with and assist the follow-on Contractor(s) in establishing the most cost-effective method for transitioning from DREN Service to replacement services without degrading existing service. The Contractor shall prepare a Contract Phase-Out Transition Plan that documents the transition methodology that will be used to phase-out the services provided under this contract. This methodology must conform to the

transition and implementation approach established by the Government for cutover to new services. At a minimum, the transition plan shall address the following:

a) The interconnection and transition methodology that will be used to transfer traffic to the new network and remove traffic from the existing DREN network;

b) Coordination and transfer of network management functions and responsibilities with the new network;

c) Description of arrangements made with follow-on WAN providers for handling special feature requirements;

d) Schedule of contract phase-out activities that will ensure timely cutover to the replacement services;

e) Points of contact that will be available to assist the Government during the transition period and provide information on DREN;

f) Description of how access to DREN facilities can be obtained, if necessary, by the follow-on WAN providers for purposes of transitioning to replacement services.

3.8.1.2 Updating, Validating, and Transferring of Support Documentation

The Contractor shall update, validate, and transfer technical data to the Government upon request. The Contractor shall ensure that all information submitted to the Government is accurate and up-to-date. This information shall include the following:

a) Inventory of service requirements for each end-user SDP;

b) Inventory of equipment at each end-user SDP; and

c) LEC circuit numbers and carrier.

3.8.2 Phase-Out

At the direction of the Government, the Contractor shall reduce and phase-out services in accordance with their Contract Phase-Out Transition Plan. The Contractor shall provide continuity of service until replacement services are available and accepted by the Government or the Government no longer desires service.

4. SECURITY

4.0 SECURITY

Information Assurance is defined as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. The security requirements for the DREN are based on the following fundamental security objectives:

a) User data entering and leaving the DREN is to be protected on network to ensure confidentiality and integrity;

b) The DREN is to maintain availability of services while under a cyber attack; and

c) Users outside the DREN will not be able to view or manipulate transport application data (e.g., network management and control data) or data used in network operations (user databases, provisioning, etc.) that is inside the DREN boundary.

The Contractor shall assist HPCMO in protecting DREN from technical, personnel and administrative threats. The Contractor shall validate that the hardware and software comply with DoD security requirements specified in this SOW.

The Contractor shall provide the Government with sufficient information to validate for itself that the vendor-developed security architecture (hardware and software), processes, procedures, and other security mechanisms are sufficient to provide the necessary levels of security specified in this SOW. The Government validation process will include comparison with other processes, procedures, and architectures used by the Government to protect user data to comply with the DoD Directive 5200.28 and DoD Instruction 5200.40. (Note: Requirement document references can be found in Section 2 of this SOW.)

The Contractor shall provide information protection within the infrastructure of the DREN against threats from hacker, criminal, foreign intelligence, and terrorist activities, consistent with the security requirements described in this SOW. The Contractor shall incorporate the security requirements and features described in this SOW into the configuration, implementation, and operation of DREN provided network service.

Security consists of three components: security service requirements, certification and accreditation support, and security operations. Security services act to protect DREN service and infrastructure resources. The Certification and Accreditation (C&A) support component identifies requirements where the Contractor shall support the Government's efforts during the C&A process. Security operations encompass the Contractor's requirement to provide for the operation and security management of all aspects of the DREN.

4.1 SECURITY SERVICE REQUIREMENT

The Contractor shall ensure availability, confidentiality, and integrity of the DREN components, support systems, and databases being maintained by the Contractor in support of DREN service. The Contractor shall provide protection to ensure the availability of provided network service to authorized users and the confidentiality of customer profile and traffic. DREN

shall satisfy security requirements described in: DoD Directive 5200.28, DoDI 5200.40. Security mechanisms will provide sufficient levels of assurance for vendor and Government security administrators, but will be as transparent as possible to the DREN user community. DREN security service requirements specified in this document are described in the following sections: Access Control, Identification and Authentication, Confidentiality and Integrity, Physical Security, and Personnel Security.

4.1.1 Access Control

The Contractor shall provide access control that prevents the unauthorized use, access, modification or destruction of any DREN resources, network management and control data, and DREN user information. Appropriate procedures for establishing and disestablishing access shall be based on need to know and the classification or sensitivity level of the information. Access control shall be enforced by the operating system based on identification and authentication techniques specified in this SOW. The Contractors network shall perform the following functions:

a) Restrict the scope of operations personnel functions performed (i.e. unauthorized combinations of session type, ports, network identification of requestor, data and time, shall be prevented);

b) Control functions performed by operations personnel based on the user ID, group membership(s), and permissions associated with the operations and or maintenance personnel (separation of privileged and unprivileged users);

c) Lock and/or terminate an interactive session after a time interval of operations personnel inactivity defined by the administrator has been exceeded. Also, require the operator to re-authenticate prior to unlocking the session; and

d) Deny operator session establishment based on any of the following conditions:

   (i) When a session is terminated (e.g., logoff occurs), the port shall drop immediately so that a subsequent user has to re-authenticate to initiate the next session; and

   (ii) Require those operations personnel to be authenticated before allowing an operator session.

4.1.2 Identification and Authentication

Identification and authentication is required to ensure that only authorized operations personnel (i.e., system administrators, network managers, operation support staff, etc) have direct access to DREN system controls, the information it processes, and the services it provides. The Contractor shall:

a) Positively identify all operations personnel authorized to access the system. As a minimum, following attributes belonging to each individual operations personnel: user id, role(s), authentication data (i.e. password determination data), and permissions;

b) Successfully authenticate each operations person before allowing that person to perform any operations functions. Identification and authentication of authorized operations personnel shall use approved NIST cryptography, Federal Information Processing Standards Publications (FIPS PUBS) Security Requirements for Cryptographic Modules (FIPS PUB 140-1), authenticated access control mechanisms (e.g., digital signature, public key cryptography based, challenge/response identification and authentication); and

c) For remote management of network components over untrusted paths (i.e. switched or networked links) the Contractor shall employ one of the following supplemental authentication mechanisms:

   (i) Token type authenticator where remote operations personnel are validated by verifying the correctness of a random number generated by the users token, i.e. One Time Password (OTP);

   (ii) Trusted centralized authentication server (such as Kerberos) to authenticate a third party operator

4.1.3 Confidentiality and Integrity

The security mechanisms implemented by the Contractor shall provide confidentiality and integrity for all DREN user information. DREN user information shall not be disclosed or modified by any entity other than the intended recipient or personnel who have a job-related requirement for access to the information as per DODD 5200.28 3/21/1988 SECURITY REQUIREMENTS FOR AUTOMATED INFORMATION SYSTEMS (AISS) section E2.1.29. Need-to-Know. The Contractor shall ensure confidentiality and integrity of DREN information through the use of DREN owned and registered ASN. Interfaces with the DREN shall be limited to Government approved NAP, MAE, and other private peering points. The integrity and security of the Contractor provided network shall be maintained at all times, including but not limited to the following events: failure of network management center, failure of individual channels or ports, failure of trunks, and failure of lines. The Contractor provided network shall:

a) Protect sensitive management/control data transmitted between network management facilities and network components from unauthorized disclosure during transmission;

b) Have the ability to detect modification of sensitive management/control data transmitted between network management facilities and network components during transmission; and

c) All IA solutions used by the contractor shall be evaluated using the Common Criteria Evaluation and Validation Scheme based on the National Information Assurance Program (NIAP) process as it may apply to the DREN requirements.

4.1.4 Physical Security

Physical security is the action taken to protect DoD information technology resources (e.g. installations, personnel, equipment, electronic media, documents, etc.) from damage, loss,

theft, or unauthorized physical access. The Contractor shall ensure physical security is in accordance with DoDD 5200.28, Security Requirements for Automated Information Systems.

4.1.5 Personnel Security

The Contractor shall ensure compliance with all DoD Personnel Security Requirements for access to Sensitive, Unclassified Information. Also, the Contractor shall ensure that Contractor personnel have the necessary Government security clearances prior to accessing the DREN.

The Contractor shall provide personnel security in accordance with DoD 5200.2-R; DoD Personnel Security Program Regulation and, as delineated in the approved Security System Authorization Agreement (SSAA) (See Section 4.2.1). Contractor personnel who are responsible for management the DREN shall successfully complete a National Agency Check (NAC), National Agency Check plus written Inquiries (NACI) as specified in DoD 5200.2-R. The Contractor shall not claim lack of an appropriate investigation as a reason for non-compliance.

4.2 CERTIFICATION AND ACCREDITATION SUPPORT

The Contractor shall support the C&A process as delineated in the approved SSAA. The Contractor shall, at the discretion of Government, provide for access to Contractor facilities and personnel involved in system design, engineering, operations, and security.

The Contractor shall support the Government's accreditation of the DREN in accordance with DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The Contractor shall perform the following service to support security certification and accreditation in accordance with DoD and Government directives:

a) Provide access to test-bed configurations that will allow security testing;

b) Assist in the testing process;

c) Provide copies of component design specifications, user manuals and results of completed security tests or vulnerability assessments;

d) Resolve problems, faults or issues that result from the testing process;

e) Develop a security operations plan defining all aspects of DREN security procedure; and

f) Develop and update Standard Operating Procedures.

The Contractor shall resolve, within 180 days, problems resulting from the security certification and accreditation process including vulnerability assessments. Resolution shall include Contractor provided assistance with security problem reports, technical investigations, testing, and regression testing procedures for correcting security defects identified during security testing activity.

4.2.1 System Security Authorization Agreement

The Contractor shall prepare and deliver a DREN SSAA to the Government. The Contractor shall also maintain and update the SSAA as requested by the Government throughout the life of the contract. The SSAA (System Security Authorization Agreement) shall reflect the physical and logical configuration and security status of the network in accordance with the DITSCAP (DODI 5200.40 12/30/97 DOD INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS. The SSAA shall provide the Government with a snapshot view of the current provided network component configuration.

4.2.2 Security Test and Evaluation Plan

The Contractor shall assist in development of a security test and evaluation (ST&E) plan. The ST&E plan shall include procedures to validate that the system satisfies security requirements specified in the approved DREN SSAA. The test plan and procedures shall be provided to the Government for approval.

4.3 SECURITY OPERATIONS

4.3.1 Network Management Data

The Contractor shall provide protection of the infrastructure and the network management data from modification while transported or contained within the infrastructure. Network management data includes accounting, configuration, fault, performance, and security management data. Such information is critical to ensuring the availability of the network.

The Contractor shall ensure the protection of the infrastructure and the network management data transported or contained within the infrastructure. The Contractor shall provide the following network management security protection measures:

a) Authentication of management traffic;

b) Network data confidentiality;

c) Identification and authentication of network personnel conducting management operations on each network component;

d) Access by authorization levels; and

e) Component port protection.

The Contractor shall assure that all management traffic is protected from compromise of confidentiality and integrity. The Contractor shall implement mechanisms to verify that routing table changes originate from routers recognized by DREN as being authoritative arbiters of network/subnetwork locations.

The Contractor shall support the Government in the procurement and implementation of security services, equipment and software that the Government deems necessary to maintain and/or enhance the security of DREN.

4.3.2 Access By Authorization Levels

The Contractor shall identify how separation of network and system access privileges of Contractor personnel is delineated, i.e., network administrator, system maintenance, business office access personnel, etc. The Contractor shall define the process for providing access privileges to Government personnel on a need to know basis. Appropriate levels of access shall be granted based on the individual's responsibility. As a minimum, the infrastructure component shall support the distinction between supervisory, operation, and maintenance privileges.

4.3.3 Service Protection

The Security mechanisms implemented by the Contractor shall protect DREN from Denial of Service attacks. Denial of Service is defined as any action or series of actions that prevents any part of a system from functioning in accordance with its intended purpose. The Contractor shall provide protection against loss or degradation of network services caused by failures/outages of network components or software and from maliciously caused attacks.

The Contractor shall provide a reporting mechanism for security incidents and security audit events that affect (or could affect) the operation and management of service provided by this contract. The following types of events shall generate an alarm: computer intrusions, attempted network intrusions, denial of service attacks, malicious logic, and probes. The Contractor shall include a definition of all alarm events in the Incident Reporting Plan and Procedures.

The Contractor shall support the Government in maintaining critical network services during and electronic attack. DREN will be responsible for taking necessary actions in response to changes in INFOCON specified in Joint Chief of Staff Memorandum CM-510-99, Information Operations Conditions. The Contractor shall support the Government in implementing changes that the Government deems appropriate during changes in INFOCON status. The Contractor shall be capable of implementing changes in network configuration that have been negotiated with the Government within 30 minutes of request (e.g., disconnecting DREN from the Internet).

The Contractor shall support the Government in protecting the DREN by implementing Government provided Access Control Lists (ACL) at any or all DREN SDPs.

The Contractor shall support the Government placement of intrusion detection sensors on the DREN. The Government, following award of this contract, will determine the exact number and location of sensors.

4.3.4 Security Incident Reporting

The Contractor shall provide security incidence reporting in accordance with the HPC CERT. Security incidence reporting addresses the following:

a) Intrusion Detection;

b) Identification of Unauthorized Users;

c) Attacks on the operations, data, and assets of DREN;

d) A process of reporting and managing security incidents;

e) A process for closing vulnerabilities identified by Incident identification;

f) Misuse detection

g) Reporting to HPC CERT.

The Contractor shall provide an Incident Reporting Plan and Procedures that describes the criteria for security incidents, process for collection and storage of security incidents, and format of information collected. The Contractor shall provide monthly reports containing information on provided network service, significant security-related events, and incidents. The Contractor shall also respond to requests for tailored security reports with Government specified information on DREN security-related events.

4.3.5 Security Vulnerabilities

The Contractor shall address security vulnerabilities by implementing procedures in accordance with the Deputy Secretary of Defense Memorandum, DoD Information Assurance Vulnerability Alert (IAVA). The Contractor shall provide a mechanism of active vulnerability analysis that will allow the Contractor and the Government to remain aware of system and network vulnerabilities and provide for the prompt reporting and correction of any vulnerability that directly or indirectly affect the infrastructure. As part of this process the Contractor shall provide normal software upgrade/patches to minimize vulnerabilities in the network at no additional cost to the Government. In addition, specific extraordinary vulnerabilities may be negotiated at the Government's request or discretion.

4.3.6 Security Audit Reporting

The Contractor shall develop and implement a program/mechanism for capturing and storing all identified DREN security audit data. All security related access events including unauthorized access attempts shall be logged. This data shall be stored in a secure manner and be available to the Government upon request.

The Contractor shall audit and log all access to security-related resources and infrastructure components. The Contractor shall maintain audit logs for usage of DREN management resources. The audit logs shall be protected against unauthorized modification and deletion. The audit logs shall include, but are not limited to, the following security-related events: unauthorized access attempts, changes to user profiles, use of security related resources/privileges, and security violations. The Contractor shall maintain the audit records on-line for 90 calendar days and archive off-line for an additional 3 years.

4.3.7 Continuity of Operations

The Contractor shall provide security management functionality for the protection of the integrity of DREN and associated resources. The Contractor shall develop a Computer/System Emergency Response Plan and Procedures. This plan will detail Contractor operating procedures, and plans for operating during emergency situations, while under malicious attacks, or other contingency situations. Contingency plans shall be developed and tested to prepare for

emergency response, backup operations, and post-disaster recovery. At a minimum, such planning shall address reconstitution for the loss of processing, storage, or transmitting of information.

4.3.8 Site-specific Security Requirements

The Contractor shall support site-specific security requirements that may be placed on the DREN depending on site location, service branch, or agency.

5. DELIVERABLES

5.0 DELIVERABLES

The Contractor shall submit deliverables as indicated in the following table:

TABLE 5-1
Deliverables

Deliverable	SOW	Deliverable	Due Date	Distribution
1	3.1.3	Monthly/Quarterly Progress Report	Monthly through IPC– Quarterly after IPC - 15th of the month	Program Office COR Contracting Office
2	3.1.4	Project Management Review	Quarterly – 15th of the month	Program Office COR Contracting Office
3	3.1.5	Annual Planning and Design Review	Yearly	Program Office COR Contracting Office
4	3.1.5.2	Annual DREN Networkers Conference	Yearly	Program Office COR
5	3.2.1	Comprehensive Implementation and Transition Plan	30 Calendar days after contract award	Program Office COR
6	3.2.1.2	Comprehensive Implementation and Transition Plan (Revised)	30 Calendar days after receipt of order for Phase II	Program Office COR
7	3.2.1.3.8	SDP Site Surveys	30 Calendar days after receipt of order	Program Office Site Representative
8	3.2.2.1	IPC Work Package (Phase I) a. IPC Test Plan b. IPC Test c. IPC Acceptance Report	15 Calendar days after Government acceptance	Program Office COR
9	3.2.2.2	Work Package (Phase II) a. Test Plan b. Test c. Acceptance Report	15 Calendar days after Government acceptance	Program Office COR
10	3.3.1.1	SDP Plan	60 Calendar days after receipt of order	Program Office COR Site Representative
11	3.3.1.1	SDP Plan Modification	30 Calendar days after receipt of order	Program Office Site Representative COR
12	3.3.1.2	"As Built" Drawings & Site System Diagrams	No later than 15 Calendar days after completion of SDP installation/ modification	Program Office Site Representative COR
13	3.3.1.4	"As Built" Drawings & Site System Diagrams	As required after completion of the SDP termination/restoration	Program Office Site Representative COR

Deliverable	SOW	Deliverable	Due Date	Distribution
14	3.4.4.1	Individual SDP Test Report	15 calendar days after test completion	Program Office COR
15	3.4.4.2	Collective SDP Test Package	15 calendar days after test completion	Program Office COR
16	3.6.3	Performance Management Data	As Required	Program Office COR
17	3.6.5	Network Management Reporting	Real Time	Available on-line to designated users
18	3.7.1.3	Service Request and Task Order tracking data	Real Time	Available on-line to designated users
19	3.7.1.3	Service Provisioning Performance Report	Monthly – 15th of every month	Program Office COR
20	3.7.2.2.1	Help Desk/Trouble ticket data	Real Time	Available on-line to designated users
21	3.7.3	Customer Care Data Reports	Real Time	Available on-line to designated users
22	3.7.4	Accounting Management Data	Update monthly	Available on-line to designated users
23	3.7.5.1	Instructional Services Training	As proposed by the Contractor	Program Office DREN Managers and Users
24	3.7.5.2, 3.7.5.3, 3.7.5.4	Technical and Telecommunications Support/ Engineering Studies	As Requested	Program Office COR
25	3.8.1.1	Contract Phase-Out Transition Plan	30 calendar days after receipt of order	Program Office COR
26	4.2	Action taken on results of Security Tests/Assessments	15 calendar days after team brief-out	Program Office COR
27	4.2	Security Operations Plans	60 calendar days after award - Updated Annually	Program Office COR
28	4.2	Standard Operating Procedures	60 calendar days after award - Updated Annually	Program Office COR
29	4.2.1	System Security Authorization Agreement	60 calendar days after receipt of order	Program Office COR
30	4.2.2	Security Test and Evaluation Plan	As required	Program Office COR
31	4.3.4	Incident Reporting Plan and Procedures	60 calendar days after award - Updated Annually	Program Office COR
32	4.3.4	Security Incident Reporting	Immediate upon detection	Program Office COR
33	4.3.6	Security Audit Reporting Data	Updated Daily	Available on-line to designated users
34	4.3.7	Computer/System Emergency Response Plan and Procedures	60 calendar days after award - Updated Annually	Available on-line to designated users
35	3.4.2.3	Packet Loss	Daily	Available on-line to designated users

Deliverable	SOW	Deliverable	Due Date	Distribution
36	3.4.3	IP Latency	Daily	Available on-line to designated users

Unless otherwise specified by the Government, all deliverables shall be submitted electronically via Email or web site in:

a) MS Word Version 7.0 (or higher as directed by the Government) with non-embedded graphics in a separate PowerPoint file; and

b) Microsoft Project application software for schedule data.

The Contractor shall provide hardcopies of deliverables upon request by the Government.

END OF ATTACHMENT 1