

Section C. PERFORMANCE BASED WORK STATEMENT

As of 7 July 2011

Contract number:	
Delivery Order Number:	

1. CONTRACTING OFFICER REPRESENTATIVE (COR).

a. Primary COR.

Name:	Douglas E. Johnson
Organization:	DDR&E HPCMP
Department of Defense Activity Address Code (DoD AAC)	
Address:	10501 Furnace Road, Suite 101 Lorton, VA 22079
Phone Number:	703 812 8205
Fax Number:	703 690 2073
E-Mail Address:	djohnson@hpcmo.hpc.mil

b. Alternate COR.

Name:	TBD
Organization:	HPCMPO
Department of Defense Activity Address Code (DoD AAC)	
Address:	10501 Furnace Road, Suite 101 Lorton, VA 22079
Phone Number:	703 812 8205
Fax Number:	
E-Mail Address:	TBD@hpcmo.hpc.mil

Table of Contents

- 1. CONTRACTING OFFICER REPRESENTATIVE (COR)..... 1**
- 2. CONTRACT TITLE..... 7**
- 3. BACKGROUND..... 7**
- 4. OBJECTIVES. 8**
 - 4.1. Synopsis of Future Network. 8**
 - 4.2. DREN III Program Objectives. 9**
- 5. SCOPE. 9**
 - 5.1. Continuity of DREN Services. 10**
 - 5.1.1. Service Locations and Duty Hours. 10**
- 6. PERFORMANCE REQUIREMENTS..... 10**
 - 6.1. Task 1. Enterprise Management Controls..... 10**
 - 6.1.1. Subtask 1. Program Management. 10**
 - 6.1.2. Subtask 2. Program Management Office. 11**
 - 6.1.3. Subtask 3. Project Management Planning and Control. 11**
 - 6.1.4. Subtask 4. Progress Reporting..... 11**
 - 6.1.5. Subtask 5. Support for the DREN Configuration Control Board (CCB). 11**
 - 6.1.6. Subtask 6. DREN Technical Advisory Panel. 12**
 - 6.1.7. Subtask 7. Operational and Management Review. 12**
 - 6.1.8. Subtask 8. Annual Planning and Design Review..... 12**
 - 6.1.9. Subtask 9. Annual DREN Networking and Security Conference. 13**
 - 6.1.10. Subtask 10. Other Conferences. 14**
 - 6.2. Task 2. Implementation and Transition..... 14**
 - 6.2.1. Subtask 1. IPC Transition Planning (Phase I). 15**
 - 6.2.2. Subtask 2. Comprehensive Implementation and Transition Plan (CITP) (Phase II). 15**
 - 6.2.2.1. Element 1. Transition. 16**
 - 6.2.2.2. Element 2. Interoperability..... 16**
 - 6.2.2.3. Element 3. Security. 17**
 - 6.2.2.4. Element 4. Implementation Schedule. 17**
 - 6.2.2.5. Element 5. Cutover..... 17**
 - 6.2.2.6. Element 6. Customer Notification..... 17**
 - 6.2.2.7. Element 7. SDP Site Surveys. 17**
 - 6.2.2.8. Element 8. Master SDP Plan. 18**
 - 6.2.2.9. Element 9. Internet Services During Transition. 18**
 - 6.3. Task 3. Implementation and Transition Actions. 18**
 - 6.3.1. Subtask 1. Phase I Actions..... 18**
 - 6.3.2. Subtask 2. Phase II Actions..... 19**

6.3.3.	Subtask 3. Transition Review.	20
6.4.	Task 4. Install, Modify, Terminate, and Restore SDPs.	20
6.4.1.	Subtask 1. Individual SDP Reports.	20
6.4.2.	Subtask 2. Acceptance Test Plan.	21
6.4.3.	Subtask 3. SDP Modification.	22
6.4.4.	Subtask 4. Acceptance Procedures.	23
6.4.5.	Subtask 5. Termination / Restoration.	23
6.5.	Task 5. Install, Modify, Terminate, and Restore Gateway Functions.	23
6.5.1.	Subtask 1. Gateways and SDPs That Perform Gateway Functions.	23
6.5.2.	Subtask 2. Internet Services and Peering.	23
6.5.3.	Subtask 3. Collocation of Government or Customer Equipment.	24
6.5.4.	Subtask 4. Peering and Network Access Points.	24
6.5.5.	Subtask 5. SDP Plans for SDPs that Perform Gateway Functions.	25
6.6.	Task 6. Disaster Recovery and Contingency.	25
6.7.	Task 7. Data Transfer Requirements.	26
6.7.1.	Subtask 1. DREN Customer Services Requirements.	26
6.7.2.	Subtask 2. Architecture Supporting Enhanced Services.	26
6.7.3.	Subtask 3. Internet Protocol Version 6.	27
6.7.4.	Subtask 4. Network Traffic Handling.	27
6.7.5.	Subtask 5. Separation and Protection.	27
6.7.6.	Subtask 6. Quality of Service.	27
6.7.7.	Subtask 7. HPCMP-Provided Network Services Support.	28
6.7.8.	Subtask 8. Flow, SNMP and SYSLOG.	28
6.8.	Task 8. SDP Characteristics.	28
6.8.1.	Subtask 1. Service Delivery.	28
6.8.2.	Subtask 2. Interface and Connectivity.	29
6.8.3.	Subtask 3. SDP-Data Transfer Rates.	31
6.9.	Task 9. SDP Functional Requirements.	32
6.9.1.	Subtask 1. SDP and Service Availability Requirements.	33
6.9.1.1.	Element 1. SDP-Availability Definitions.	33
6.9.1.2.	Element 2. Determination of SDP Service Availability.	33
6.9.1.3.	Element 3. Billing Credits for SDP Outages.	34
6.9.2.	Subtask 2. Network Performance: Packet Loss.	34
6.9.3.	Subtask 3. Network Performance: Latency.	35
6.9.4.	Subtask 4. Network Performance: Availability.	35
6.9.4.1.	Element 1. Network Availability Determination.	35
6.9.4.2.	Element 2 Network Availability Billing Credits.	37
6.10.	Task 10. Contractor Verification of Services.	37

6.10.1.	Subtask 1. Individual SDP Test.....	37
6.10.2.	Subtask 2. Aggregate SDP Test.	38
6.10.3.	Subtask 3. Government Verification of Services.	38
6.11.	Task 11. Local Connectivity from SDP Sites to Secondary Sites.	38
6.12.	Task 12. Ethernet and VLAN Services.	39
6.13.	Task 13. Internet Protocol Service.	40
6.13.1.	Subtask 1. Multiple IP Networks and Services.	40
6.13.2.	Subtask 2. Public-External IP Network.....	41
6.13.3.	Subtask 3. DoD-Only IP Network.	41
6.13.4.	Subtask 4. Internet-Access Network or Service.	42
6.13.5.	Subtask 5. DMZ IP Network.....	42
6.13.6.	Subtask 6. Outreach.....	42
6.13.7.	Subtask 7. Gateways.....	42
6.13.8.	Subtask 8. Internet Services and Rich Peering.....	43
6.13.9.	Subtask 9. Addressing.	43
6.13.10.	Subtask 10. Routing.	44
6.13.11.	Subtask 11. Autonomous System Numbers.	44
6.13.12.	Subtask 12. Customer Routing.	44
6.13.13.	Subtask 13. IP Multicast.....	45
6.14.	Task 14. Optical Services.	45
6.15.	Task 15. Evolution of Existing Services.	46
6.15.1.	Subtask 1. Technology Insertion.....	46
6.15.2.	Subtask 2. Upgrades.	46
6.15.3.	Subtask 3. Technical Refresh and Life Cycle Engineering Support.	47
6.15.4.	Subtask 4. Government versus Contractor Initiated Proposals.....	47
6.15.4.1.	Element 1. Government Initiated.....	47
6.15.4.2.	Element 2. Contractor Initiated.	47
6.16.	Task 16. Contractor Simulation Environments and Test Labs.	47
6.17.	Task 17. Network Management.....	48
6.17.1.	Subtask 1. Network Supervision and Maintenance.	48
6.17.2.	Subtask 2. Fault Management.....	48
6.17.2.1.	Element 1. Fault Management at Network Level.....	49
6.17.2.2.	Element 2. Problem and Fault Isolation – Ethernet Services.	49
6.17.2.3.	Element 3. Problem and Fault Isolation – Internet Protocol Service.....	49
6.17.2.4.	Element 4. Problem and Fault Isolation – Optical Services.....	49
6.17.2.5.	Element 5. Problem and Fault Isolation – SDP Utilized as Gateways.	50
6.18.	Task 18. Performance Management.	50
6.18.1.	Subtask 1. Performance Measurement and Validation.	50

6.19.	Task 19. Configuration Management.	51
6.20.	Task 20. Network Management Reporting.....	52
6.21.	Task 21. Network Visibility and Customer Tools Sets.....	53
6.22.	Task 22. Domain Name Service.....	53
6.23.	Task 23. Customer Care.	53
6.23.1.	Subtask 1. Service Provisioning.	53
6.23.1.1.	Element 1. Service Requests and Delivery Orders.	54
6.23.1.1.1.	Subelement 1. Service Requests.....	54
6.23.1.1.2.	Subelement 2. Delivery Orders.....	54
6.23.2.	Subtask 2. Provisioning of Service Requests and Delivery Orders.....	54
6.23.2.1.	Element 1. Provisioning of Service Requests.	54
6.23.2.2.	Element 2. Provisioning of Delivery Orders.	55
6.23.2.3.	Element 3. Expedited Delivery Orders.....	55
6.23.2.4.	Element 4. Service Request and Delivery Order Tracking.....	56
6.24.	Task 24. Service and Problem Management.....	57
6.24.1.	Subtask 1. Help Desk / Network Operations Center.....	57
6.24.1.1.	Element 1. Customer Problem Management.....	58
6.24.1.2.	Element 2. Trouble Resolution.....	58
6.24.1.3.	Element 3. Problem Escalation.	59
6.24.2.	Subtask 2. Record Keeping.	60
6.25.	Task 25. Customer Care Data and Reports.	61
6.26.	Task 26. Accounting Management.	63
6.27.	Task 27. Customer Support and Instructional Services.	63
6.27.1.	Subtask 1. Instructional Services.	63
6.27.2.	Subtask 2. Telecommunications-Related Support.	64
6.27.3.	Subtask 3. Engineering Studies.....	64
6.27.4.	Subtask 4. Customer Care Tools.	64
6.28.	Task 28. Contract Phase Out.	65
6.28.1.	Subtask 1. Planning and Engineering Support.	65
6.28.1.1.	Element 1. Development of Contract Phase-out Transition Plan.....	65
6.28.1.2.	Element 2. Updating, Validating, and Transferring of Support Documentation.	66
6.29.	Task 29. Phase Out.	66
7.	PERFORMANCE STANDARDS:.....	66
8.	INCENTIVES.	72
9.	PLACE OF PERFORMANCE.	72
10.	PERIOD OF PERFORMANCE.	72
11.	DELIVERY SCHEDULE.....	73
12.	SECURITY.....	78

12.1.	Organization.	78
12.1.1.	Facility Clearance.....	78
12.1.2.	Personnel.	79
12.1.3.	Control of Contractor Personnel.	79
12.2.	DREN Security Requirements.	80
12.3.	Access Control.	80
12.4.	Non-Contractor Network Resource Access.....	81
12.5.	Identification and Authentication.....	81
12.6.	Confidentiality and Integrity.....	82
12.7.	Physical Security.	82
12.8.	Personnel Security.	82
12.9.	Security Enhancing Network Features.	83
12.10.	Certification and Accreditation (C&A) support.....	83
12.11.	DIACAP package.....	84
12.12.	Security Test and Evaluation Plan.....	86
12.13.	Security Operations.	86
12.13.1.	Network Management Data.	86
12.13.2.	Access by Authorization Levels.	87
12.13.3.	Service Protection.	87
12.13.4.	Security Incident Reporting.....	88
12.13.5.	Security Vulnerabilities.....	88
12.13.6.	Security Audit Reporting.....	89
12.13.7.	Continuity of Operations.	89
12.13.8.	Site-Specific Security Requirements.	89
ATTACHMENT A		90
ATTACHMENT B		94
ATTACHMENT C		109
ATTACHMENT D		111
ATTACHMENT E		113
ATTACHMENT F.....		116
ATTACHMENT G.....		124

2. CONTRACT TITLE.

Defense Research Engineering Network III (DREN III) Contract.

3. BACKGROUND.

The High Performance Computing Modernization Program (HPCMP) was established in 1992 in response to Congressional direction to modernize Department of Defense (DoD) high performance computing (supercomputing) capabilities. The HPCMP was assembled out of a collection of small, high performance computing departments, each with a rich history of supercomputing experience that had independently evolved within the DoD's Military Services.

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 missions. The Defense Research Engineering Network (DREN), a component of the HPCMP, provides high performance wide area network services in support of DoD scientists and engineers and provides network and security support to other Federal Agencies where it's in the best interest of the Government.

DREN is a sophisticated, robust, high performance communications network that incorporates the best capabilities of both DoD and the commercial telecommunications infrastructure. DREN has become DoD's premier Wide Area Network (WAN) communication service provider for research, development, test and evaluation.

DREN enables scientists and engineers at defense laboratories, test centers, universities, and industry sites throughout the United States to use HPCMP computing resources. DREN provides secure gateways to existing Federal and civilian networks, allowing access to the program's resource centers from a wide variety of facilities. The network links customer sites to HPCMP's DoD Supercomputing Resource Centers (DSRC) and Affiliated Resource Centers (ARC). Additional background material on HPCMP can be found at <http://www.hpcmo.hpc.mil>.

The networking services of DREN are currently provided by a virtual WAN built on a commercial communications network and provide digital data transfer services between defined Service Delivery Points (SDP) that comprise DREN. SDPs are specified in terms of bandwidth requirements, physical interface, and transport protocols.

DREN's Internet Protocol (IP version 6 and version 4) service for video, audio, imaging, and digital data connects to other research and academic networks at private and public Internet Exchange Points (IXP). DREN today has a mix of more than 225 sites at DS-3 through OC-48 rates. The HPCMP will continue to upgrade DREN by establishing connectivity at new sites, increasing bandwidth at existing sites, as well as inserting technology across the network.

4. OBJECTIVES.

The objective of this contract encompasses state-of-the-art WAN data transfer and related services to support DREN customers. DREN's primary mission is to support the research and development communities of the DoD. The primary customer support within DoD focuses on Science and Technology (S&T), Test and Evaluation (T&E), and Modeling and Simulation (M&S). DREN also provides transit, network, and security support to other Federal Agencies and academia.

4.1. Synopsis of Future Network.

DREN III is expected to be a sophisticated, robust, high performance WAN employing the latest commercially available technology. DREN is a high performance network, serving its customers with the latest services available in the industry – with technological refreshment infusion ongoing through the life of the contract. The DREN III network is expected to continue advancing this concept systematically throughout its operational life.

The DREN III network will be required to provide services based on Ethernet and optical technology with protocols including IPv6 and IPv4. Optical capabilities and services represent the way forward for high capacity and high performance as well as scalable internal and external interchange for an ever increasing demand.

DREN services shall be delivered to a DREN customer site at a physical interface called a SDP. The SDP is where the provider's service network ends and the customer premises network begins (see Figure 6.8.1a). Interconnectivity is required internally between DREN locations as well as externally with DoD, Federal, research, academic, and other Government-designated networks at both private and public IXPs. All DREN customer locations require the ability to reach the Internet via DREN connectivity which will be provided by the Contractor.

The DREN network is engineered to support applications to include, but not limited to, video, audio, imaging, distributed storage, and digital data services. Demands of the DREN III network will be even higher as it must be engineered to meet the ever-increasing complexity of the DREN customers' mission requirements in a distributed and interactive computing environment while meeting more stringent security and separation requirements.

The architecture must incorporate a complex design of multiple routing and security domains in order to address the needs of groups of DREN customers and applications that have a consistent over-arching governance – Information Assurance (IA) governance in particular – and other relationships requiring different levels of separation and protection of the traffic from other traffic traversing the network. These groups are hereinafter referred to as "collectives". Further, more exclusive subsets of these groups of applications or connections--referred to as "communities of interest"--require separation, connectivity, or traffic handling refinements within these collectives, adding some

complexity to the overall design. (For a more detailed discussion of “separation and protection” and “collectives” refer to Attachment D and Attachment E, respectively.)

The current DREN serves more than 225 service delivery points. Cutover to the replacement network is expected to be essentially transparent to the existing DREN customers. The current SDP sites and their associated bandwidths are identified in Attachment B.

4.2. DREN III Program Objectives.

Data transport service requirements for DREN III are derived from customer requirements for remote computer operations and the need to engage in collaborative initiatives in distributed and interactive environments. Many DREN customers employ applications that require enormous computing capabilities. The corresponding network traffic to support these HPC and distributed collaborative environment capabilities is projected to require constant increases in bandwidth throughout the life of the contract.

Therefore, DREN III services will support the following:

- a. Collaboration and effective pooling of resources.
- b. Real-time scientific visualization.
- c. Rapid access to multi-media libraries and large distributed computational resources using meta-computing approaches.
- d. Access for DREN sites to the Internet, national research and education networks, national and regional optical networks, and various R&D network test beds.
- e. Connectivity between DoD Shared Resource Centers for large scale distributed computing, distributed mass storage file systems, and archival storage.
- f. Very large single stream data rates between user desktops and large scale computational systems, databases, libraries as well as other systems.
- g. Special dedicated connectivity between members of a Collective or Community.
- h. Shorter term dedicated (virtual) connectivity builds for special projects, exercises, and demonstrations.

5. SCOPE.

DREN is a “SERVICES” contract providing a robust, high capacity, low latency network capability in support of DoD S&T, Research Development Test & Evaluation (RDT&E) Communities. The service shall be engineered to support applications to include, but not be limited to, video, audio, imaging, distributed storage, and digital data connections provided both internally among directly-connected

DREN customers and externally to other DoD, Federal, research and academic networks both at private and public IXP.

5.1. Continuity of DREN Services.

The Contractor shall provide all labor, management, supervision, supplies, materials, equipment, and tools not otherwise provided as Government furnished property to perform the non-personal services required to acquire state of the art WAN services to support DREN III. Current DREN networking capability is being provided under the DREN telecommunications services contract administered by the Contracting Officer. This procurement will enable continuation of DREN network capability.

5.1.1. Service Locations and Duty Hours.

The Contractor shall provide WAN services on a 24 hour, seven (7) day a week basis. Locations supported under the current DREN contract are specified in Attachment B, although service to all existing locations may not be ordered under this solicitation. Additional locations may be added as fully negotiated modifications to the base contract. Locations can be both within and outside CONUS.

6. PERFORMANCE REQUIREMENTS.

The Contractor shall deliver the services set forth in this PWS pursuant to issuance of delivery orders. The Contractor, acting independently, 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 PWS. The Contractor shall comply with the standards identified in Attachment F in performance of the services provided under this PWS.

6.1. Task 1. Enterprise Management Controls.

6.1.1. Subtask 1. Program Management.

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 shall 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 PWS shall be interpreted to mean an authorized Government representative as designated by the Contracting Officer.

6.1.2. Subtask 2. 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. The Contractor shall provide a central coordination point for all DREN problems not resolved at the local site or DREN Network Operations Center (NOC).

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 be fully operational within thirty (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 PMO and NOC shall have video-teleconferencing (VTC) capabilities compatible with VTC capabilities used by the HPCMP Office (HPCMPO).

6.1.3. Subtask 3. Project Management Planning and Control.

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

6.1.4. Subtask 4. Progress Reporting.

The Contractor shall participate in weekly status meetings with the Government on accepted and proposed network modifications and deliver progress reports on a quarterly basis. The quarterly progress report will identify significant activities, problems, and accomplishments during the preceding three months. The quarterly report shall also identify significant areas of technology improvement within the Contractor's core infrastructure.

6.1.5. Subtask 5. Support for the DREN Configuration Control Board (CCB).

The Contractor shall support preparation for and execution of DREN CCB meetings by:

- a. Assisting in the development of weekly meeting agendas by tracking unresolved issues;
- b. Planning and tracking of approved network modifications and upgrades;
- c. Planning and tracking all SDP installations, SDP plans, as well as SDP upgrades, modifications and terminations;
- d. Generating meeting minutes and addressing action items.

All Configuration Management records must be kept current and accurate.

6.1.6. Subtask 6. DREN Technical Advisory Panel.

The DREN Technical Advisory Panel (TAP) is a working group under the DREN Project Manager (PM). The TAP consists of HPCMP personnel, Service and key site representatives, and significant community of interest representation. Proposed major network modifications, upgrades and improvements shall be vetted through the DREN TAP for discussion before final approval by the HPCMPO DREN PM and DREN contracting officer. The Contractor shall participate and assist in TAP activities as needed. 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 TAP meetings shall take place at a location determined by the Government.

6.1.7. Subtask 7. Operational and Management Review.

The Contractor shall conduct regular quarterly reviews that shall address the current status of technical and programmatic progress, significant infrastructure changes within the DREN boundaries, and significant technology changes within the larger network infrastructure. Each review, at a minimum, shall focus on achievements since the last review, the 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.

6.1.8. Subtask 8. Annual Planning and Design 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. Equipment lifecycle status;
- c. Network and security metrics;
- d. Growth analyses and resource allocations;
- e. Planned transmission network growth;
- f. Trend analyses and projections;
- g. Security measures and impact;
- h. Advanced planning data and contingency plans;
- i. Interfaces with other networks; and
- j. Analyses of changes in technology and/or potential service improvements that may enhance DREN services or reduce costs.

Annual design reviews shall address the current status of technical and programmatic progress, significant infrastructure changes within the DREN boundaries, and significant technology changes within the larger network infrastructure.

The Contractor shall provide a restricted web site to post the above data and present its capability to the Government for approval.

6.1.9. Subtask 9. Annual DREN Networking and Security 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, and 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 at no additional costs to the Government:

- 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 DREN network access for attendees; and
- g. Develop a record of the conference and provide the record to attendees.

The Contractor will recover costs associated with this conference through the registration fees of the attendees. The Contractor shall make every effort to minimize the conference fees. After the conclusion of the conference the Contractor shall provide a record of the conference attendees, fees collected, and expenditures in support of the annual Conference. This conference shall take place at a mutually agreed location. The first conference location will be provided at contract award. Each consecutive year's location will be announced at the conclusion of the previous annual conference.

6.1.10. Subtask 10. Other Conferences.

The Contractor shall coordinate other Conferences, which shall be separately priced, on an as negotiated basis. Once ordered, the Contractor shall perform the following tasks to support such conferences:

- a. Obtain the facility;
- b. Arrange for scheduled speakers;
- c. Notify 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.

Such Conferences shall take place at a location approved by the Government.

6.2. Task 2. Implementation and Transition.

The Contractor shall perform the necessary planning and actions to successfully implement and transition the DREN SDPs. During transition, the Contractor shall establish and maintain full interoperability with the existing DREN at Contractor-provided inter-network gateways (traffic exchange points) until all sites are transitioned. During and subsequent to transition, the Contractor shall establish and maintain high performance Internet transit service, as well as regional IP transit, via peering arrangements with major Tier 1 and Tier 2 service providers.

The Contractor shall manage the transition of an existing DREN SDP for which a Delivery Order is issued to the DREN III. The transition of existing DREN SDPs shall be completed in two phases. Phase I shall include those sites identified for the Initial Performance Capability (IPC) demonstration; Phase II shall include all other existing SDPs for which a Delivery Order is issued. The Contractor shall provide for Government approval, an individual plan for each phase that identifies all task activities and schedule milestones associated with the activities described below. After contract award, the Government will provide to the Contractor all releasable engineering and technical data from the existing contract to assist in development of these plans.

6.2.1. Subtask 1. IPC Transition Planning (Phase I).

The Contractor shall develop and submit the general approach, along with a timeline and site selections for the IPC demonstration. A proposed plan for the IPC demonstration shall be submitted by the Contractor in addition to the Proposal in response to this solicitation. The proposed plan shall outline processes to be used and projected schedules or timelines and should demonstrate the Contractor's reasonable, logical, and realistic approach to the overall transition. The plan shall also specifically include the Contractor's approach to selection and transition of ten (10) initial sites for Government approval. The Contractor shall identify geographically disparate sites from the categories listed in Attachment B. The ten sites selected shall contain at a minimum two (2) from category A, two (2) from category B, three (3) from category C, as well as one (1) new DREN III IXP. The remaining two (2) sites can be selected from any of the above.

An updated draft of the IPC plan shall be submitted within thirty (30) calendar days following contract award. The Government will review and provide comments to the Contractor on the draft plan not later than five (5) working days following receipt of the plan. The Contractor shall submit a final IPC plan within fifteen (15) days following receipt of Government comments. The Government will provide comments or accept the final Plan within five (5) working days following receipt of the Plan.

The Contractor's plan shall include sections detailing the testing procedures, applications and equipment to be used for acceptance testing of individual SDPs, as well as for an aggregate test. The section addressing an aggregate SDP test plan shall detail procedures, applications and equipment for simultaneous operation of the full set of all IPC SDPs. At a minimum, the procedures shall include:

- a. Demonstration of the operation of the Digital Data Transfer Services to comply with subtask 6.4.2.
- b. Demonstration of successful completion of routine service configurations as described in Subelement 6.23.1.1.1;
- c. 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.

6.2.2. Subtask 2. Comprehensive Implementation and Transition Plan (CITP) (Phase II).

The Contractor shall prepare and submit a CITP detailing the planning, processes, and activities for Phase II transition. A draft CITP shall be due within thirty (30) days after acceptance of the final report following successful completion of the IPC demonstration. The Government shall review and provide comments to the Contractor on the draft plan not later than five (5) working days following receipt of the plan. The Contractor shall submit a Final CITP within fifteen (15) days following receipt of Government comments. The Government will provide comments or accept the final plan within five (5) working days following receipt of the Plan.

Throughout Phase II, for tracking purposes, the Contractor shall continue to update and revise (as applicable) appropriate sections of the Final CITP to account for the work being performed and completed.

The CITP shall include, as a minimum, the elements described below.

6.2.2.1. Element 1. Transition.

The Contractor’s plan shall provide details for transitioning services from the existing contract 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 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 gateways interconnecting the new DREN III—including Internet transit service and regional IP transit—with the existing DREN II—including Internet transit service and regional IP transit—to ensure a transparent transition with minimum effects on service quality and availability.

The plan shall include gateways supporting high performance data transfer greater than or commensurate with existing capacity today between DREN and other non-Contractor networks, both Government and non-Government, to ensure minimum impact on service quality and availability during transition. The plan shall include 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.

6.2.2.2. Element 2. Interoperability.

The Contractor’s plan shall provide detail for interoperating with 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, and domain names that will be used for the DREN community between internal and external networks. The Contractor shall be responsible for managing the administration of these items. The Contractor shall establish and maintain high performance Internet transit service, as well as regional IP transit, via peering arrangements with major Tier 1 and Tier 2 service providers. The Contractor also shall provide detail for interoperating with other Government and non-Government networks. The Contractor shall

describe gateways to support high performance data transfer between DREN and other Government and non-Government networks.

6.2.2.3. Element 3. Security.

The Contractor's plan shall detail the approach for implementing the security requirements detailed in Paragraph 12 of this PWS.

6.2.2.4. Element 4. Implementation Schedule.

The Contractor's plan shall provide an implementation schedule for completing the transition. 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, to include establishing Internet transit service. 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.

6.2.2.5. Element 5. Cutover.

The Contractor shall describe an overall approach for cutover of services at all SDPs. The Contractor shall consider impact to communities of interest under consideration, performance issues, and other concerns such as security.

6.2.2.6. Element 6. Customer Notification.

The Contractor shall identify its approach for notifying site communications personnel of pending service cutovers and of pending Contractor-conducted testing thirty (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.

6.2.2.7. Element 7. SDP Site Surveys.

Upon execution of a delivery order by the Contracting Officer, the Contractor shall conduct CONUS and OCONUS site surveys at each SDP as identified in Attachment B. The Contractor shall contact the site POC at least fifteen (15) calendar days prior to the survey. The Government will provide a list of site POC's after contract award. Site survey results shall be posted for access by HPCMP management and network personnel within five (5) working days following the survey.

6.2.2.8. Element 8. Master SDP Plan.

The Contractor shall provide a Master SDP Plan that documents all standard requirements and processes for installing equipment in buildings and on a facility to support delivery of DREN service to a location. The Master SDP Plan shall detail all vendor and industry standards pertaining to installation and maintenance of the SDP and site and equipment requirements, e.g., power, HVAC, plumbing, floor loading, storage, etc, as identified in Attachment G.

The Contractor shall also address standard processes and procedures proposed to support upgrades, e.g., WAN connections, new interfaces or services, to an existing SDP; for problem identification and resolution; termination or restoration of an existing SDP; training, etc. The Master SDP Plan shall reference and shall support the SDP Acceptance Test Plan described in Subtask 6.4.2.

A Draft Master SDP Plan shall be submitted as part of the Draft CITP within thirty (30) days after acceptance of the IPC Demonstration Report. The Government shall respond with comments and recommendations. The Contractor shall submit a proposed Final Master SDP Plan within fifteen (15) calendar days of receiving comments and recommendations from the Government.

The Contractor shall update, revise and maintain the Master SDP Plan throughout the life of the contract.

6.2.2.9. Element 9. Internet Services During Transition.

During the transition the Contractor shall provide high performance Internet transit service, as well as regional IP transit, in accordance with requirements established in Subtask 6.13.7, Gateways, to support DREN sites during and after transition. The data transfer rates at these IXPs shall be sufficient to support intra-regional traffic exchanges between the DREN and the Internet and between the DREN and other Tier 1 and Tier 2 networks. The Contractor shall not use another Tier 1 network, i.e. the network provider from whom a DREN customer is transitioning, for transit of DREN traffic to another Tier 1 or Tier 2 ISP during the transition.

6.3. Task 3. Implementation and Transition Actions.

6.3.1. Subtask 1. Phase I Actions.

The IPC will demonstrate and prove the Contractor's proposed process for the installation and testing of the block of SDPs, as well as the initial ramp-up of other capabilities such as on-line reporting of the DREN services environment. The Contractor shall utilize only Contractor-provided resources; no Government CPE shall be utilized. Native IP multicast, both IPv6 and IPv4, shall be available during this phase.

Upon direction of the Contracting Officer, the Contractor shall execute the approved IPC Plan that governs the actions associated with the installation of the set of SDPs identified for the IPC demonstration.

The Government may delay the start of the aggregate SDP test, at no further cost to the Government, but such delay may not exceed ten (10) workdays.

Upon completion of the activities described above, the Contractor shall prepare and post for Government approval an IPC Acceptance Report documenting all results of the execution of the test(s). This report shall document the full completion of the IPC demonstration and at a minimum shall include a copy of acceptance reports for each of the individual SDPs, the aggregate SDP test and other Government-approved tests. The Contractor will be reimbursed at the completion of an acceptable IPC and upon Government acceptance of the IPC demonstration report. During the IPC, the Government will collaborate with the Contractor to prioritize the remaining DREN II sites identified as candidates for transition in Phase II to the DREN III network. However, no additional Delivery Orders will be issued by the Government until the IPC demonstration has been accepted by the Government.

6.3.2. Subtask 2. Phase II Actions.

Following completion and acceptance of the IPC demonstration report and upon direction of the Contracting Officer, the Contractor shall execute the revised and approved CITP that governs the actions associated with the installation of the Phase II set of SDPs.

The Government may issue one or more delivery orders to initiate the transition of SDPs that currently comprise the DREN. The transition of these remaining sites is collectively referred to as Phase II. Phase II provides for the implementation and testing of existing SDPs to be transitioned and any additional DREN service capabilities not completed in conjunction with the IPC demonstration. A discrete delivery order will be issued for an individual site, i.e., one site per delivery order, although multiple customers or enclaves may be supported by an SDP at an individual site. Delivery orders for the transition of SDPs during Phase II may be issued individually or in groups or bundles, i.e., multiple delivery orders.

The Contractor shall install and document ordered SDPs during Phase II in accordance with the Government-approved Final Master SDP Plan detailed in 6.2.2.8 and implement the Acceptance Test plan for individual SDPs detailed in the CITP. The results of such testing shall govern acceptance of each individual SDP during this phase. Upon completion of the SDP Acceptance Test, the Contractor shall submit Individual SDP Reports to address site-specific details, including any variance from the standards documented in the Master SDP Plan. The Individual SDP Report shall be due within fifteen (15) Calendar days of completion of the test as outlined in section 6.4.1. Individual SDP Reports for the IPC set of SDPs shall be created or updated and submitted in accordance with the Final Master SDP Plan prior to acceptance of any Phase II Individual SDP Reports.

Throughout Phase II, the Contractor shall continue to update and revise (as applicable) the CITP to account for the work being performed and completed.

6.3.3. Subtask 3. Transition Review.

The Contractor shall monitor and report on the efficiency and effectiveness of transition on a monthly basis. In addition, the Contractor shall conduct weekly status meetings on the progress of transition until all existing DREN SDPs have been transitioned to the DREN III contract. These weekly status meetings shall be conducted by VTC or conference bridge provided by the Contractor.

After transition of the SDPs identified for the IPC, the Contractor shall conduct regular quarterly reviews until Phase II transition is complete. Each review, at a minimum, shall focus on achievements since the last review, the 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.

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

6.4. Task 4. Install, Modify, Terminate, and Restore SDPs.

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

6.4.1. Subtask 1. Individual SDP Reports.

Upon execution of a delivery order or delivery order modification by the Contracting Officer, the Contractor shall conduct as necessary a site survey and post the results for access by HPCMP management and network personnel within five (5) working days following the survey.

A Draft Individual SDP Report shall be submitted no later than fifteen (15) calendar days after completion of the SDP Acceptance Test. The Draft Individual SDP Report shall address site-specific details, including any variance from the standards documented in the Master SDP Plan and incorporated elements and standards identified in Attachment G. The Draft Individual SDP Report shall also include an as-built diagram of all equipment and cabling to support the SDP and the results of the

SDP Acceptance Test. The Government shall review and provide comments and recommendations. The Contractor shall submit a proposed Final Individual SDP Report within fifteen (15) calendar days of receiving comments and recommendations from the Government. .

The Individual SDP Report shall be submitted in an electronic form agreed to by the Government and either encrypted or password protected for transmission purposes only. The Individual SDP Report shall be updated and maintained throughout the life of the contract including documenting modifications to the SDP.

6.4.2. Subtask 2. Acceptance Test Plan.

When a new SDP is ordered, the Contractor shall validate the proper installation and operation of a DREN SDP with its ordered service and interfaces in accordance with the approved SDP Acceptance Test Plan. The objective is to ensure that an ordered DREN SDP with one or more interfaces is configured correctly and will operate in accordance with DREN III service requirements. Successful testing in accordance with the approved plan will result in an "active" SDP with services and interfaces that meet the requirements specified in this PWS.

The Acceptance Test Plan, originally created during transition and detailed in the CITP, shall identify all reference SDP(s), e.g., SDP 0, and any additional reference test points on the Contractor network. The Test Plan shall specify the physical location and describe the configuration(s) and capabilities of all reference SDPs and test points. The Test Plan shall identify all applications or hardware supported at each of the reference SDPs and test points. The Test Plan shall also describe the signal flow(s) between the SDP under testing and the reference SDPs or test points that may be utilized during testing.

The Acceptance Test Plan shall identify the location(s) and personnel involved in acceptance testing, identifying conditions under which an individual or agency might be involved or not involved in testing.

The Test Plan shall describe initial acceptance testing of an SDP and testing conducted to accept an upgrade or new service ordered for an existing SDP, to include personnel, applications and hardware involved in each.

The Acceptance Test Plan shall specify the information included in the report generated for each SDP under testing. The Contractor shall submit an acceptance test report for each SDP within five (5) calendar days following testing. At a minimum, the Test Plan shall specify and the report shall include:

- a. Day and date of testing.
- b. Reference testing location(s).
- c. Domain Name Service (DNS) name of the SDP under testing.

- d. The latitude and longitude of the SDP under testing.
- e. Line-of-sight (LOS) distance in kilometers between the reference testing location(s) and the SDP under testing.
- f. Type of service(s) or interface(s) tested.
- g. Test equipment or applications used.
- h. Service Performance, e.g., latency, throughput, packet loss, etc., to be measured.
- i. Metrics captured.

The Acceptance Test Plan shall provide a table detailing each test performed during the initial Acceptance Test following installation of an SDP. The table shall identify the PWS reference and description for each characteristic of a service or interface to be tested.

The Contractor shall submit a sample test plan for Government approval with this proposal.

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, at no additional cost to the Government, all or any portions of the SDP Acceptance Test in the event that the SDP fails to satisfy any of the test criteria.

6.4.3. Subtask 3. SDP Modification.

The Contractor shall provide a description of required changes for each SDP modification or upgrade action. In the event that a site survey is required to document the required changes, the Contractor shall contact the Government-identified Site POC at least fifteen (15) calendar days prior to the survey to schedule the visit.

Each description shall address the following:

- a. Transmission media construction such as cabling, repeaters, and conduits.
- b. Building modifications, if any, necessary to install equipment and run cables.
- c. Storage space requirements.
- d. Staging area requirements.
- e. An analysis of the impact on active SDPs at this site and at other sites, including identification of any actions needed to prevent negative impact.

On completion of modification or upgrade the Contractor shall submit "as built" site drawings and diagrams.

6.4.4. Subtask 4. Acceptance Procedures.

Following installation of the SDP, the Contractor shall execute the acceptance tests in accordance with the Government-approved SDP Acceptance Testing procedures.

6.4.5. Subtask 5. Termination / Restoration.

Upon request of the Government, the Contractor shall deactivate and remove the SDP. The Contractor shall identify that equipment or cabling that shall be removed and any that shall be abandoned in place.

In the event that a site survey is required to complete the planning, the Contractor should contact the Government-identified site POC at least fifteen (15) calendar days prior to the survey to schedule the visit.

6.5. Task 5. Install, Modify, Terminate, and Restore Gateway Functions.

6.5.1. Subtask 1. Gateways and SDPs That Perform Gateway Functions.

The Contractor shall provide gateway functions at locations between independent networks in accordance with requirements in this section as well as sections 6.7.7 and 6.13.7. Gateway functions include routing, isolation through access lists or filtering, and collocation of Government equipment to support HPCMP-provided services. Gateway routing and filtering functions range from basic layer 3 separation between routing domains with minimal protections within a collective to extensive security boundary implementation of separation and protection between collectives. These functions may occur at an SDP or similar connection implemented at a boundary between DREN and other networks, e.g. Internet Exchange Points (IXPs), private peering locations, Internet Transit Service provider connections; or the function may occur at a core location in DREN where collectives or routing domains coincide.

Where the proposed architecture requires a gateway function, between two or more DREN collectives or routing domains, or at connections between a DREN network and an outside entity, the Contractor shall support the installation and delivery of equipment, up to and including an SDP, as well as Government-provided equipment to enable HPCMP-provided network services as part of those gateway functions in accordance with the following requirements.

6.5.2. Subtask 2. Internet Services and Peering.

Collocation agreements at IXPs and other private exchanges shall be prepared by the Contractor for Government approval and signature. The Contractor shall operate as the Government's technical representative in maintaining the peering and proper IP prefix advertisements and, if necessary, shall notify all existing peering partners in the event of outages or configuration changes involving DREN or other networks or consortiums supported by DREN. The Contractor shall maintain

current data and status of all peering connections and prefix exchanges for view by the HPCMPO and DREN Customers.

The Contractor shall further be able to isolate DREN or other Federal networks or consortium supported by DREN from any network or exchange point by making changes to associated routing tables, access control lists, or any other contractor-managed configurations upon direction from the Government (See Paragraph 12 Security.) and provide timely support for HPCMP-directed security countermeasures in keeping with network-enhanced security strategies.

6.5.3. Subtask 3. Collocation of Government or Customer Equipment.

The Contractor shall prepare collocation agreements, if required, for non-exclusive license to use facilities at locations supporting gateways or SDPs that perform gateway functions. The Contractor shall provide at a minimum 38-inches (22 Rack Units) of contiguous rack space to support collocation of Government Furnished Equipment (GFE), e.g., firewall, security protection devices, Active Measurement Program (AMP) node, etc., and cabling (hereinafter the "Equipment" for the purpose of interconnecting the Equipment with the SDP and/or the external entities to support security, testing, monitoring, etc. Government-designated personnel will have access to the collocation space twenty-four (24) hours a day, seven (7) days a week with reasonable advance notice. The Contractor shall provide basic Plain Old Telephone Service (POTS) to support out-of-band management access securely to the Equipment.

The Government will provide the Contractor a detailed description and schematic drawing of the Equipment to be placed in the collocation space when gateway service is ordered. Requirements for temporary or other storage of equipment; interconnection of Equipment with equipment or services of any local access provider other than the Contractor; HVAC and conditioned, uninterruptible power support; or enclosure of rack or floor space shall be defined on an individual case basis. Pricing shall be inclusive of all applicable charges including collocation charges; power charges, if applicable; cross-connect fees, etc. The Government will not provide or make available space within the collocation space to any third party.

6.5.4. Subtask 4. Peering and Network Access Points.

The DREN and other Federal networks supported by DREN will use Government-owned and registered ASNs for purposes of identification in Border Gateway Protocol (BGP) peering relationships with other networks at SDPs that perform Gateway functions such as peering or connecting to external entities. The Government will control peering relationships at Network Access Points (NAP) and other private exchanges.

The Contractor shall operate as the Government's technical representative in maintaining the peering and proper route advertisements and, if necessary, shall notify all existing peering partners in the event of outages or configuration changes involving DREN or other Federal networks supported by

DREN. Pricing shall be inclusive of all applicable charges including any charges, e.g., collocation, levied at network access points or private peering points.

The Contractor shall provide transit to any Tier 1 Internet Service Provider that is not directly peering with DREN. The Contractor shall maintain, and exchange with others, routing information of all networks attached to and peering with DREN. The Contractor shall maintain current status about DREN in public registries, e.g., PeeringDB and RADb

The Contractor shall be able to isolate DREN or other Federal networks supported by DREN from any network or exchange point, or make changes to associated routing tables, and access control lists, or take other security measures upon direction from the Government (see Paragraph 12 Security.)

6.5.5. Subtask 5. SDP Plans for SDPs that Perform Gateway Functions.

The Contractor shall provide an SDP Plan for an SDP that performs gateway functions. This gateway SDP Plan shall include the detailed description and schematic drawing of the GFE in the collocation space. The SDP Plan also shall identify agreements for temporary or other term storage of equipment; and describe in detail all associated cross-connects and other associated SDP plan components.

SDP component details shall include, but are not limited to, inter-connection of GFE or Contractor-provided equipment with equipment or services of any local access provider other than the Contractor; HVAC and conditioned, uninterruptible power support provided by the facility; any enclosure of rack or floor space; original and upgrades or modifications to the SDP and GFE in the collocation space; hardware inventory, e.g., a “show chassis” report from the SDP device(s); an elevation view drawing of the equipment rack(s) or cabinet(s) in which the SDP and GFE is installed; cross-connect drawings depicting wiring cross-connections between the SDP equipment and components and GFE or Contractor-provided equipment or any equipment or services of any local access provider other than the Contractor; cable management, to include cross-connect drawings depicting wiring cross-connections between SDP equipment and other components, i.e., jumpers on a distribution frame, building entrance terminals, etc., for both the gateway service and the commercial basic (POTS) telephone service supporting out-of-band management access to the SDP and GFE.

6.6. Task 6. Disaster Recovery and Contingency.

The Contractor shall exert its best effort 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 protect the transmission services in accordance with the security requirements of this PWS. In the event of a disaster, the Contractor shall implement the Computer / System Emergency Response Plan as described in subparagraph 12.13.7 Continuity of Operations.

6.7. Task 7. Data Transfer Requirements.

6.7.1. Subtask 1. DREN Customer Services Requirements.

DREN services shall be delivered to the customer via the SDP on an appropriate interface in accordance to the service ordered. The Ethernet service shall have an industry-standard connector and signal format commensurate with the service rate ordered as identified in Table 6.8.2a. The customer interface for an optical service shall have an industry standard connector accepting a single-mode fiber carrying one or more lambdas in the C-Band.

Ethernet-based services shall be provided to the customer using either direct connection (untagged) or Virtual Local Area Network (VLAN) tagging in accordance with IEEE 802.1Q standards and extensions such as IEEE 802.1AE, 802.1ad, 802.1ah and 802.1Qay. Basic DREN services delivered over the Ethernet customer interface shall include publicly routable IP connectivity as well as the enabling of virtually private enterprise and Community of Interest connections. Ethernet or IP traffic transmitted into an SDP through an Ethernet interface will be routed by the most optimal path over the network to other SDPs supporting Ethernet or IP packets.

Over the life of the contract any site may also order optical interfaces and services, to include Optical Wavelength Service (OWS), other Optical Transport Unit (OTU)/ Generic Framing Procedure (GFP) transport, and Lambda Transport. An optically enabled SDP shall support multiple optical services over a single WAN access circuit.

6.7.2. Subtask 2. Architecture Supporting Enhanced Services.

The Government may request at one or more sites enhanced services such as MPLS, Infiniband, or end-to-end services such as various flavors of circuit cross connects (CCC) or circuit emulation to support unique customer requirements. Upon receiving such requirements, the expectation is these services are routine in scope but enhanced from the viewpoint of a tailored setup. Upon receiving these types of requirements, the Contractor shall provide a more detailed engineering solution.

Enhanced network service plans include: network connectivity, customer interfaces, data transfer rates or limitations, exceptions or limitations to meeting governing performance or availability requirements, details on addressing or other protocol information, Contractor verification of service, unique network support or management criteria, and customer support management and reporting.

Although these services will be addressed on an individual case basis, the Contractor shall describe how their network architecture will support implementation and functional management of these services. Attention shall be given not only to the capabilities the architecture provides but also the management of service implementations, protocols and technologies to enhance the delivery and organization of the services, and testing and visibility tools to support the management of customer connections.

6.7.3. Subtask 3. Internet Protocol Version 6.

DREN is identified as an IPv6 network with IPv4 legacy support. Therefore, all systems, software, and equipment supporting the DREN network and its services shall handle IPv6 in an equivalent or better way than current IPv4 capabilities, performance, and security. No systems, software, or equipment shall be deployed on the DREN that does not meet this requirement. Additionally, all network management shall be enabled using IPv6.

6.7.4. Subtask 4. Network Traffic Handling.

The equipment chosen for the SDP must be able to distinguish between traffic destined for different enclaves at the site, provide appropriate separation and protection between types of services or connections being delivered at that SDP (e.g. collective, community of interest, or enterprise), and differentiate traffic by class and quality of service (See Attachment D and Attachment E).

IP traffic transmitted into the DREN network through the interface or VLAN supporting IP Services at an SDP will be routed over the network in accordance with functional requirements outlined in Task 6.13. The network shall provide end-to-end transport of Ethernet frames or IP packets of at least 9000 bytes plus tagging and transport protocol overhead without fragmentation. The only exception is for IPv4 packets where the egress SDP interface has a smaller MTU, in which case standard fragmentation (including path MTU discovery – ref. RFC 1191) can occur.

6.7.5. Subtask 5. Separation and Protection.

Separation and Protection as defined in Attachment D, must be implemented in accordance with the appropriate strength on any and all DREN services as dictated by the HPCMPO or its designate in order to maintain proper security posture, accreditation boundaries, and necessary technical functionality in support of mission.

6.7.6. Subtask 6. Quality of Service.

End to end Quality of Service (QoS) controls shall be implemented across the DREN WAN. At the Ethernet layer, 802.1p Class of Service (CoS) shall be supported. At the IP layer, the network shall support RFC 2475 DiffServ, including the Expedited Forwarding (EF) and Assured Forwarding (AF) Per-Hop Behavior (PHB). If carried over other protocols at layers below IP, different classes of service must be preserved, using DiffServ aware MPLS (MPLS-TE / MPLS-TP), PBB-TE, or similar, depending on the implementation.

At every SDP, it shall be possible to assign class of service controls to individual 802.1Q VLANs, to allow for example a certain priority or amount of bandwidth to be assigned to each VLAN. Where routing occurs, each router at the IP layer shall be able to accept packets that have already been tagged with DiffServ Code Point (DSCP) values and apply the corresponding DiffServ PHB's to them.

The router shall also be able to initially classify and tag traffic with DSCP values based on combinations of protocol, ports, and source and destination addresses.

6.7.7. Subtask 7. HPCMP-Provided Network Services Support.

The overall network architecture shall support and facilitate HPCMP-provided network services such as Computer Network Defense, Security Posture and Strategy (as described in Paragraph 12 Security.), performance testing, and service status and verification. The Contractor shall support the ability of the Government to instrument network-based services at any SDP or gateway location to include integrated strategic defense, DREN active measurement program, traffic analysis using flow data, and monitoring.

6.7.8. Subtask 8. Flow, SNMP and SYSLOG.

Every DREN router and switch shall generate and export flow records (NetFlow v5, NetFlow v9, IPFIX, sFlow RFC 3176, sFlow 5 or similar). A real time copy of the flow records from all routers and switches shall be forwarded to one Government specified destination address. Sampled flow collection is sufficient, but shall support a sampling rate of 1 in 512 or finer.

Similarly, the Contractor shall forward raw SYSLOG messages for every DREN router and switch to at least one Government specified destination address.

The Contractor shall provide SNMP read access to all routers, switches, and other SNMP manageable devices in the network.

6.8. Task 8. SDP Characteristics.

Service Delivery Points shall operate under the following characteristics and guidelines.

6.8.1. Subtask 1. Service Delivery.

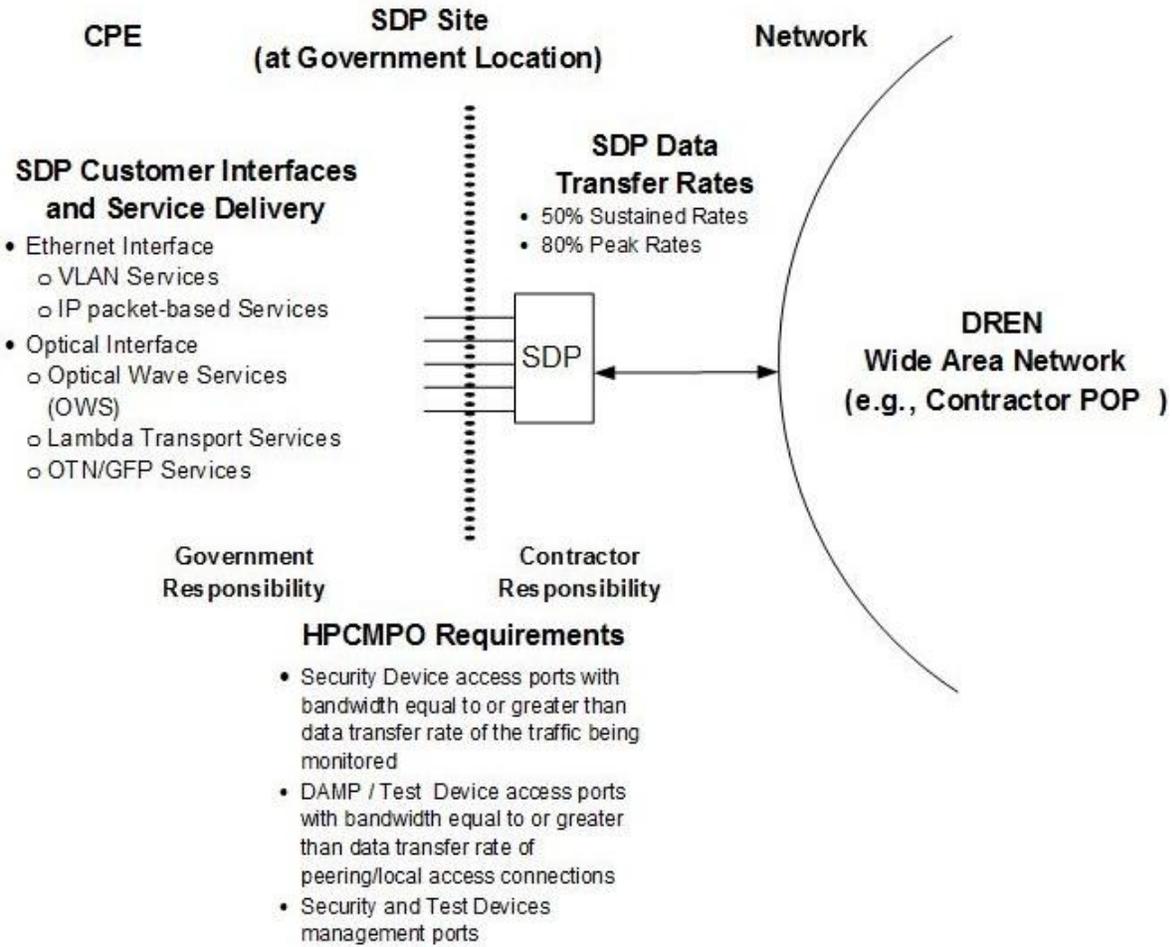
The Contractor shall provide continuous, uninterrupted concurrent multi-protocol digital data transfer services between active SDPs.

SDP services provide the interface between the SDP and the HPCMPO or User CPE, based on interface standards and data transfer rate. The customer(s) may order one or more interfaces on a SDP to support Ethernet service delivery (which includes both VLAN service and IP packet-based service delivered over Ethernet) and/or Optical services according to the applicable service requirements outlined in this PWS.

In addition, as outlined in Subtask 6.7.7, the HPCMPO has a requirement for access to data traversing the network as well as the ability to inject test traffic into the network at key locations. The Contractor shall provide or facilitate access for these HPCMP-provided services at the SDP or elsewhere in the Contractor network to support integrated security devices, DREN Active Measurement Program (DAMP) devices, and other systems as defined by the HPCMP.

An SDP is further defined by sustained and peak data transfer rates, which specify the 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

Figure 6.8.1a SDP Characteristics



to other SDPs. These SDP characteristics are illustrated in Figure 6.8.1a.

6.8.2. Subtask 2. Interface and Connectivity.

SDPs with Ethernet service shall be capable of supporting delivery of DREN services to a customer using one or more of the physical interfaces listed in Table 6.8.2a and in accordance with standards set forth in Attachment G. The Contractor shall not require the Government to install separate SDPs to support specific interfaces or types of traffic defined as DREN Service; for example, the Contractor shall not require separate SDPs at an SDP site for IP traffic.

With the possible exception of delivery of “enhanced services”, as defined in subtask 6.7.2, all interfaces supporting SDP Services shall be either based on appropriate twisted pair or fiber interface standards. The Contractor shall not employ equipment supporting SDP services requiring coaxial cable Government equipment interfaces.

Table 6.8.2a SDP Ethernet Service Interfaces

Interface	Description
100BASE-FX	Fiber Fast Ethernet
4x100BASE-FX	Fiber Fast Ethernet – 4 ports
8x100BASE-FX	Fiber Fast Ethernet – 8 ports
100BASE-TX/1000BASE-T	Copper Fast/Gigabit Ethernet (Auto)
4x100BASE-TX/1000BASE-T	Copper Fast/Gigabit Ethernet (Auto) – 4 ports
8x100BASE-TX/1000BASE-T	Copper Fast/Gigabit Ethernet (Auto) – 8 ports
1000BASE-SX	Fiber Gigabit Ethernet (Short Range)
4x1000BASE-SX	Fiber Gigabit Ethernet (Short Range) – 4 ports
8x1000BASE-SX	Fiber Gigabit Ethernet (Short Range) – 8 ports
1000BASE-LX	Fiber Gigabit Ethernet (Long Range)
4x1000BASE-LX	Fiber Gigabit Ethernet (Long Range) – 4 ports
8x1000BASE-LX	Fiber Gigabit Ethernet (Long Range) – 8 ports
10GBASE-T	Copper 10-Gigabit Ethernet (Twisted Pair)
10GBASE-CX4	Copper 10-Gigabit Ethernet (IB Cable)
10GSFP+Cu	Copper 10-Gigabit Ethernet (Direct Attach)
4x10GSFP+Cu	Copper 10-Gigabit Ethernet (Direct Attach) – 4 ports
8x10GSFP+Cu	Copper 10-Gigabit Ethernet (Direct Attach) – 8 ports
10GBASE-SR	Fiber 10-Gigabit Ethernet (Short Range)
4x10GBASE-SR	Fiber 10-Gigabit Ethernet (Short Range) – 4 ports
8x10GBASE-SR	Fiber 10-Gigabit Ethernet (Short Range) – 8 ports
10GBASE-LR	Fiber 10-Gigabit Ethernet (Long Range)
4x10GBASE-LR	Fiber 10-Gigabit Ethernet (Long Range) – 4 ports
8x10GBASE-LR	Fiber 10-Gigabit Ethernet (Long Range) – 8 ports

Interface	Description
40GBASE-CR4	Copper 40-Gigabit Ethernet
40GBASE-SR4	Fiber 40-Gigabit Ethernet (Short Range)
40GBASE-LR4	Fiber 40-Gigabit Ethernet (Long Range)
100GBASE-CR10	Copper 100-Gigabit Ethernet
100GBASE-SR10	Fiber 100-Gigabit Ethernet (Short Range)
100GBASE-LR10	Fiber 100-Gigabit Ethernet (Long Range)

Optical services will be delivered to the customer over single mode fiber (SMF) using an industry standard connector (e.g. LC) using one of the interfaces listed in Table 6.8.2b . An interface configured for Optical Wavelength Service (OWS) will accept a standard SONET Short Reach signal at 1310 nm and deliver it to an OWS optical interface on a remote SDP as specified in 6.14 Task 14. Optical Services. Optical Transport Network (OTN) interfaces will accept a G.709 framed signal at the specified OTU rate and deliver it to a matching remote OTN interface. Lambda transport will accept one or more lambdas in the C-Band and pass them transparently to a remote Lambda Transport interface. OWS and OTN interfaces allow for electrical regeneration along the path. Lambda Transport allows for C-Band amplification but no electrical regeneration, as the modulation format may be unspecified. As such it is understood that the effective reach of a Lambda Transport connection may be limited.

Table 6.8.2b SDP Optical Service Interfaces

Interface	Description
SONET OC48 SR SMF	OC48 OWS
SONET OC192 SR SMF	OC192 OWS
G.709 OTU1 SMF	2.7 Gbps OTN
G.709 OTU2 SMF	10.7 Gbps OTN
G.709 OTU3 SMF	43 Gbps OTN
G.709 OTU4 SMF	112 Gbps OTN
SMF C-Band	Lambda Transport

6.8.3. Subtask 3. 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 the sustained / peak data rate pairs listed in Table 6.8.3a. These rates apply to all user traffic at an SDP, regardless of protocol or SDP Service at the originating or terminating SDP.

The rates specified, although in some cases readily identified with existing last mile delivery technologies, are not intended to be exact bit rates but rather approach common levels of data rates. Many of the rates identified may be delivered by different technologies at slightly different specific data rates dependent upon the technology, media, or protocol format or standard. The Contractor may elect to proffer a single technology and rates, e.g., Ethernet and commercial rates, such as 100/1000/10000 Mbps, or only SONET rates, or may offer a combination of technologies and rates. The Contractor shall identify the exact data rate or alternative rate or technology identifier on a per-SDP basis in any pricing tables in order to clarify the service level being offered. The access circuit connecting the SDP must support data transfer at a rate equal to or greater than the line rate specified in Table 6.8.3a. For example, “622 service” may be provisioned via Gigabit Ethernet should the offeror elect to do so. As new technologies become commercially available in each SDP market, the pricing should then be provided accordingly.

Table 6.8.3a SDP Sustained and Peak Rate Combinations

	SDP Line Rate								
	45 Mbps	100 Mbps	155 Mbps	622 Mbps	1 Gbps	2.4 Gbps	10 Gbps	40 Gbps	100 Gbps
SDP Peak Rates [Mbps] (80% of line speed)	36	80	124	498	800	1920	8000	32000	80000
SDP Sustained Rates [Mbps] (50% of line speed)	23	50	78	311	500	1200	5000	20000	50000

The sustained and peak rates shall apply to all user data transmitted through an SDP, excluding protocol overhead needed for framing or routing the user data to the destination user device.

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.

6.9. Task 9. 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.
- g. The Contractor shall manage active SDPs in a manner that permits the Government to utilize the SDP performance capabilities on demand.

6.9.1. Subtask 1. SDP and Service Availability Requirements.

Each active SDP shall experience no more than 30 minutes of outage per month. Billing credits for such outages should be provided according to the schedule specified in Table 6.9.1a. The definitions used for determining SDP availability are provided below.

6.9.1.1. Element 1. SDP-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.

6.9.1.2. Element 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.

6.9.1.3. Element 3. Billing Credits for SDP Outages.

Table 6.9.1a 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 %
10 hours up to, but not including, 12 hours	30.0 %
12hours up to, but not including, 14 hours	35.0 %
14 hours up to, but not including, 16 hours	40.0 %
16 hours up to, but not including, 18 hours	45.0 %
Over 18 + hours	50.0 %

* % Credit applies to SDP monthly recurring charges

6.9.2. Subtask 2. Network 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 shall 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 shall 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 shall use a standards compliant, off-the-shelf TCP/IP implementation in the computer at each endpoint. This test shall be at least 10 minutes in duration. The IPC demonstration shall include but is not limited to a wide-area (preferably coast-to-coast) test between two of the highest bandwidth sites. This IPC demonstration shall include tests where the computers are connected via appropriately-sized-Ethernet interfaces. 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 C.

The loss of IP packets submitted to the network shall not exceed one tenth of 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” by the Government. The Contractor shall measure packet loss and report results daily.

6.9.3. Subtask 3. Network Performance: Latency.

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 or VLAN services deployed at two SDPs shall be governed by distance between those SDPs according to the following rule:

$$\text{Round Trip Time (in milliseconds)} = (0.02 \times \text{Inter-SDP distance in kilometers}) + 20$$

Inter-SDP distance shall be established as line-of-sight. For example, roundtrip delay for IP traffic entering the network between two SDPs 3000 kilometers apart must not exceed 80 milliseconds. Traffic between all SDP’s 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.

6.9.4. Subtask 4. Network Performance: Availability

The aggregation of all DREN services, comprising services to all SDPs, will be required to meet a Network Availability of 0.999 (99.9%) for each calendar month. This is a measurement of end-to-end services calculated as a percentage of the total reporting time of a standard month for which a service is operationally available to the user.

6.9.4.1. Element 1. Network Availability Determination

Network availability refers to the fraction (or percentage) of total possible uptime achieved in a period and is calculated by the following industry standard formula, modified to represent the aggregation of all SDPs on the network:

$$\text{Network Availability} = \left\{ \frac{\text{Total Availability} - \text{Aggregate Unavailability}}{\text{Total Availability}} \right\}$$

Total Availability (TA) refers to the total time (in minutes) in a calendar month that the sum of all SDPs in the network should be available. This is derived from multiplying the standard number of minutes in a month by the number of SDPs on the network. Hence, SDP count, not bandwidth, is the

factor in the Network Availability computation. The number of SDPs in service at the end of the month shall determine the number of SDPs in the total Network Availability computation.

$$\textit{Total Availability} = \frac{\textit{\# minutes}}{\textit{calendar month}} \times \textit{\# of SDPs}$$

“Calendar month” by convention is 365 24-hour days in a calendar year divided by 12 months, or 730 hours. Using minute resolution (730 hr X 60 min/hr) means one month equals 43,800 minutes.

Aggregate Unavailability (AU) refers to the total (qualified) time of service unavailability aggregated from all SDPs in the calculation. The following unavailability calculation guidelines shall apply:

- a. The first five (5) calendar days of service outages (a total of 5 X 24 = 120 hours) resulting directly from Acts of God shall not be included in the aggregation of service unavailability minutes. For this purpose Acts of God are considered to be severe outages resulting from
 - i. Tornadoic and/or hurricane force destruction, including the associated flooding;
 - ii. Earthquake destruction;
 - iii. Other violent acts of nature rendering unusual, inordinate destruction to telecommunication facilities. For outages resulting from these acts, the Contracting Officer will be the final arbitrator in allowing the exclusion of these conditions from the Network Availability computation.
- b. The first eighteen (18) hours of any SDP outage will not be counted against the Network Availability.

The following is an illustrative computation of the Network Availability applying the foregoing guidelines:

Suppose for example a calendar month, equaling a total of 43,800 minutes, ends with 100 SDPs on the network, provides a **Total Availability** of 4,380,000 minutes.

$$\textit{Total Availability} = \frac{43,800 \textit{ min}}{\textit{calendar month}} \times \textit{\# 100 SDPs} = 4,380,000 \textit{ min}$$

In our illustration, 5 SDPs experienced service unavailability totaling 124 hours and 29 minutes. However, the first 18 hours of outage for each SDP is NOT included, reducing the aggregate qualified service unavailability by 90 hours (5 SDPs X 18 hours), bringing the total **Aggregate Unavailability** to 34 hours and 29 minutes (or 2,069 minutes).

A 6th SDP in the illustration had an outage due directly to a hurricane, resulting in four (4) 24 hour days plus 3 additional hours of outage, totaling 99 hours of service outage at the affected location. This outage is within the severe outage qualification and therefore is also NOT included in the

availability computation, leaving the Aggregate (qualified) Unavailability at 2,069 minutes. The resultant calculation using the above parameters reads:

$$\text{Network Availability} = \left\{ \frac{4,380,000 (TA) - 2069 (AU)}{4,380,000 (TA)} \right\} = 0.99953$$

The 99.953% availability for this illustration is greater than the minimum standard, resulting in no billing credits for that period under the Network Availability requirement.

6.9.4.2. Element 2 Network Availability Billing Credits

Failure to meet the monthly aggregate Network Availability Requirement of 0.999 (99.9%) will result in Billing Credits issued by the Contractor per the following schedule. Credits escalate on substandard aggregate Network Availability of every one tenth of one percent by which this parameter fails to meet the minimum standard. The first step in the schedule is the interval below 99.9%, in which one percent of the total network billing is due as a credit. Similar calculations apply to subsequent increments below 99.8%. Billing credits for Network Availability should be provided according to Table 6.9.4a.

Table 6.9.4a Determination of Outage Credits for Network Availability

Aggregate Network Availability	Credit Applied to Billing*
X ≥ 99.9%	No Credit Due
99.8% ≤ X < 99.9%	1% X total mo. network billing
X < 99.8% [In 0.1% steps]	An additional 1% of total network billing for each full or partial step.

* % Credit applies to Total monthly recurring charges

Total outage credits for failure to meet the Network Availability standard are limited to fifty percent (50%) of the monthly recurring charge for the total network.

Outage Credits for individual SDP Availability are calculated as shown in Table 6.9.1a, and are independently calculated from Network Availability. For monthly billing purposes, SDP outage credits are additive to the billing credits associated with Network Availability.

6.10. Task 10. Contractor Verification of Services.

6.10.1. Subtask 1. Individual SDP Test.

Upon installation or when ordered by the Government, the Contractor shall execute acceptance testing in accordance with the SDP Acceptance Test Plan outlined in Subtask 6.4.2 Acceptance Test Plan and approved by the Government.

The Government reserves the right to witness the Individual SDP tests. The Government will provide notification to the Contractor of intent to witness an individual SDP test and specify participating Government personnel.

Upon completion of the requested test the Contractor shall submit an update to the Individual SDP Report for the SDP under test documenting all results of the execution of the test(s).

6.10.2. Subtask 2. Aggregate SDP Test.

As a means of examining the effects and impacts of the simultaneous operation of sets of active SDPs, the Contractor shall perform an aggregate SDP test, i.e., tests of sets of SDPs. The aggregate SDP Test Plan and Test Report for the IPC shall not be separately priced. After the IPC Test Report has been accepted by the Government, each aggregate SDP test ordered by the Government shall be separately priced. The Contractor shall create an Aggregate SDP Test Plan for Government approval prior to performing an aggregate SDP test. The Aggregate SDP Test Plan shall detail the SDPs to be included in the test being conducted, as well as the procedures, applications and equipment for simultaneous operation of all SDPs under test. The Contractor shall utilize only Contractor-provided resources; no Government Contractor Premise Equipment shall be utilized. Such tests shall, as a minimum, address the following test considerations:

- a. Demonstration of the operation of the Digital Data Transfer Services to comply with this subtask.
- b. 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.
- c. The Government will witness the Aggregate SDP Test. The Contractor shall ensure the Government is able to view results in real time remotely.
- d. Upon completion of the aggregate SDP test, the Contractor shall submit an aggregate SDP test report documenting all results of the execution of the test(s).

6.10.3. Subtask 3. Government Verification of Services.

The Government will have the right to access SDP equipment for independent testing and evaluation activities with 24 hours advance notice to the Contractor.

6.11. Task 11. Local Connectivity from SDP Sites to Secondary Sites.

Upon request, the Contractor shall provide and manage connectivity between an SDP site and secondary sites. Connectivity between an SDP and a secondary site shall be provided from the SDP interface, to a demarcation point at the secondary DREN site. Connectivity between an SDP and a secondary site or among secondary sites may be provisioned via Metropolitan Area Networks (MAN). Responsibility for link utilization and performance of non-Contractor-provided equipment and cabling

between the SDP and secondary sites will be negotiated on a case-by-case basis. The Contractor shall provide management; routine maintenance; trouble isolation among Government, Contractor, and Local Exchange Carrier (LEC) or MAN facilities; providing restoration of the link or service.

The Contractor shall provide the Government with a proposal for connectivity at the request of the Government, which shall include but not be limited to: all engineering services, materials (not including equipment), the services to be provided for the connectivity, and the service performance levels to be provided. The Government will have the right to accept or refuse the Contractor's proposal. If accepted, the Contractor shall update the SDP Plan(s) and related sub-plans for the SDP at which the local connectivity service is to be provided and any secondary sites where Contractor-provided equipment will be installed and maintained.

6.12. Task 12. Ethernet and VLAN Services.

The Contractor shall provide wide area Ethernet services between sites and to core gateways, delivered over 802.1Q "VLANs" at the customer interface on the SDP, using native transport or a tunneling mechanism (e.g. VPLS or equivalent technology). The DREN NOC shall configure each VLAN, as specified by the HPCMPO, to a given set of customer or core interfaces. The network shall support hundreds of such VLANs. Each VLAN shall be totally isolated (logically separate) from all other VLANs, and shall be protected from accidental leakage between them through automated and/or administrative mechanisms.

Each VLAN could be point-to-point, point-to-multipoint, or multipoint-to-multipoint. Multiple VLANs can appear to the customer on a single tagged interface, or be delivered on separate untagged interfaces.

Every SDP shall be able to accept Ethernet frames containing customer VLAN tags, and carry those tags unmodified across the WAN (e.g. QinQ 802.1ad, or PBB 802.1ah). Support for PBB-TE (802.1Qay) is also required.

Every Ethernet device in DREN shall be capable of supporting 9000 byte "jumbo frames" (or larger). Individual VLANs may be configured as having either 1500 byte or 9000 byte frames.

The network shall support Ethernet broadcast and multicast. The implementation must minimize how much broadcast and multicast traffic is replicated over a given access circuit for each VLAN. Bifurcation shall occur within the backbone, not at the edge (SDP).

In support of IPv6 multicast, all layer 2 switches in the network shall support MLD snooping, and understand / support MLDv2. In support of IPv4 multicast, all layer 2 switches in the network shall support IGMP snooping, and understand / support IGMPv3.

The Ethernet service shall optionally support MAC address filtering or access control, bandwidth limiting keyed to a single Ethernet MAC address, or bandwidth limiting keyed to the entire VLAN logical interface.

Dynamic or automated provisioning of VLANs by HPCMPO is desired, but manual provisioning of VLANs by the DREN NOC is allowed where new VLANS shall be added to existing interfaces within four hours.

Ethernet services shall be delivered over a separate physical Ethernet interface or over an additional logical interface on the same physical Ethernet interface as managed IP services for a given DREN customer. From the DREN customer’s perspective, they can reach both Ethernet and managed IP services over a set of VLANs on a single customer Ethernet interface to the SDP, or can choose to reach these services over separate Ethernet interfaces.

Encrypted VLANs is an enhanced service, to provide additional protection of sensitive data traversing certain VLANs. If the offerors solution has the capability the Contractor should describe how their architecture supports 802.1AE MAC security (aka MACsec) or equivalent encryption mechanisms.

6.13. Task 13. Internet Protocol Service.

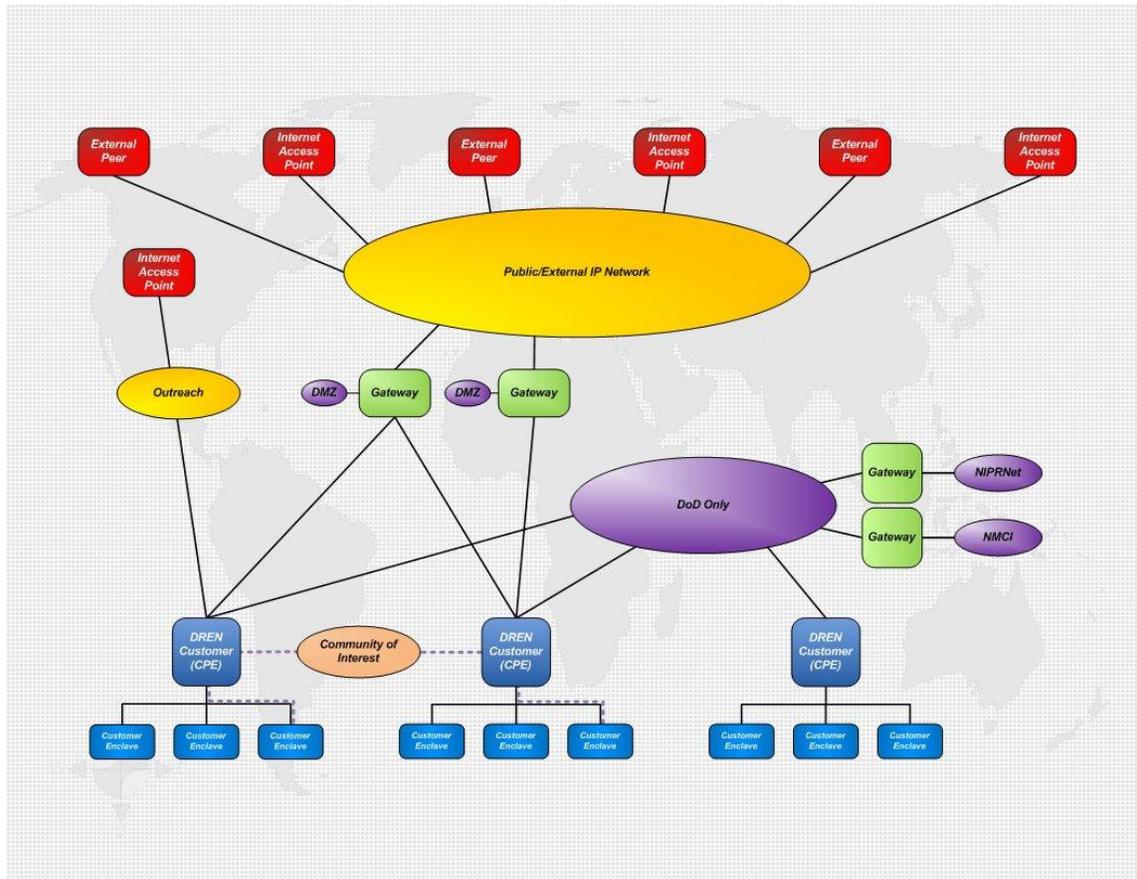
Internet Protocol version 6 (IPv6) and version 4 (IPv4) services, both unicast and multicast, shall provide the full suite of capabilities as outlined below:

6.13.1. Subtask 1. Multiple IP Networks and Services.

The DREN IP service must operate as rich, adaptive, dynamic autonomous routing environments independent of any other network and shall be divided and managed as multiple IP networks or inter-networks, interconnected internally and to external IP networks using IP gateways (routers). Each IP network or service has a unique function or security posture. A collection of networks and services operating within the same security boundary or under the same IA governance is referred to as a “collective” with salient features as detailed in Attachment E. DREN shall support multiple collectives—including but not limited to the DoD and Internet collectives.

The following illustration is one view of how these multiple collectives, IP networks, and gateways are related:

Figure 6.13.1a Notional Collectives / Networks / Gateways Architecture



6.13.2. Subtask 2. Public-External IP Network.

The Public-External IP network resides within the Internet collective and exists in support of peering with all external non-DoD networks. It operates as a traditional Tier-1 or Tier-2 ISP, following all Internet best practices, carries no default route, provides the full suite of IP services (unicast, multicast, IPv4, IPv6, and jumbo), and is the transit network for all DREN connectivity to the Internet and non-DoD private peers. Routing mechanisms shall be optimized for low latency (i.e. tuned with metrics and using “hot potato” routing) to IP destinations.

6.13.3. Subtask 3. DoD-Only IP Network.

The DoD-only IP network resides in the DoD collective and exists to route IP traffic between DoD customers and to other DoD networks. It has internal peering relationships with DoD customers, and external peering relationships with other DoD networks (NIPRnet, NMCI, etc.), and carries ONLY DoD routes. It shall conform to all DREN latency and performance requirements.

6.13.4. Subtask 4. Internet-Access Network or Service.

The Internet-Access network resides in the DoD collective and exists to support DREN customer access to the Internet. Its only function is to provide IP transport between DREN customer networks and gateways to the Internet and other DREN collectives. It does not provide transport between DREN customers directly. This may operate as a set of point to point virtual links between customers and the nearest gateway(s) located elsewhere in the DREN core.

6.13.5. Subtask 5. DMZ IP Network.

The DMZ IP network resides in the DoD collective and exists to support systems and servers that provide public-facing services to the Internet via extensions to individual DREN sites.

6.13.6. Subtask 6. Outreach.

The Outreach network which resides in the Internet collective provides direct non-attributable (IPs not DoD related) access from DREN sites to the Internet via connectivity directly to the Tier 1 Internet Transit Service as defined in sections 6.13.8 and 6.13.9.

6.13.7. Subtask 7. Gateways.

Gateways are devices and functions that interconnect independent IP networks. Gateways are required to provide interconnections between the IP networks on DREN and to external (off-DREN) networks. Gateways provide a path for IP packets to be transported between any of these IP networks. This applies to IPv6 and IPv4, unicast and multicast.

Gateways shall perform IP routing and forwarding functions based on Internet best current practice and conventions, and operate standard gateway protocols for the exchange of routing information. The exterior gateway protocol shall be BGP4, and standard interior gateway protocols (IGPs) shall be used for all internal routing. The IGPs include OSPF, ISIS, and/or I-BGP. In some instances, static routing can be appropriate. PIMv2 shall be used for multicast routing. MSDP shall provide source discovery for external IPv4 multicast domains.

Gateways shall perform various filtering functions. In particular, the ingress filtering specified in BCP84 shall be fully supported. Additional filters are required for each IP network instance on DREN. Gateway filters shall be able to whitelist or blacklist any prefix or individual host IP address. Management and control of such filters shall use automated or dynamic mechanisms to affect network-wide updates within 60 seconds.

Gateways shall have the ability to redirect any traffic based on source address, destination address, protocol, ports, and other attributes. Gateways shall support BGP FlowSpec as specified in RFC 5575.

Within DREN, a sufficient number of gateways or gateway functions shall be provided to meet the requirements, service levels, and separations specified here and elsewhere in this document. Gateways on DREN must:

- a. connect internal IP networks within a collective
- b. connect internal IP networks to external networks within the same collective
- c. connect between collectives

Gateways shall be regionally distributed in order to minimize latency between the various IP networks, and to keep traffic within-region where possible. Gateway functions shall adhere to the separation requirements described in Attachment E.

Government owned and operated devices that perform various HPCMP functions (security, performance measurement, monitoring, etc.) will be co-located with the DREN gateways as outlined in sections 6.5 and 6.7.7. Every gateway shall include a “half rack” of space and associated HVAC, conditioned power, and UPS for HPCMP devices. Additional Ethernet interfaces (up to 8 interfaces supporting bandwidth equal to or greater than the peering bandwidth) shall be provided for connecting to the HPCMP devices.

6.13.8. Subtask 8. Internet Services and Rich Peering.

The Contractor shall provide high performance Internet transit service to any domain not in a direct peer relationship with DREN. The Contractor shall provide a regionalized Internet Service solution, to include peering locations with other Tier 1 and Tier 2 networks providing the shortest path from DREN sources of traffic to the Internet and from Internet sources to the DREN, and to facilitate the local exchange of intra-regional traffic between DREN and the Internet and between DREN and other Tier 1 and Tier 2 networks. The Contractor shall provide data transfer rates at each location sufficient to support intra-regional traffic exchanges between the DREN and the Internet and between the DREN and other Tier 1 and Tier 2 networks.

The Government may also order SDPs at metropolitan area IXPs to facilitate rich direct or public peering with service and content providers. All public IXPs and ISP connections shall be routed appropriately within the Public-External IP network and made available at gateway locations across DREN as directed by the Government. Traffic destined to public-facing DoD servers shall be directed to the DMZ collective according to the HPCMP security and routing posture and strategy.

6.13.9. Subtask 9. Addressing.

The Contractor shall use Government-provided addresses for DREN specific functions within the DREN accreditation boundary. DoD designated addresses shall not be used on network elements shared by other customers of the Provider or that fall outside the DREN accreditation boundary. In those cases, either the Agency requesting the service or the Contractor shall provide address space.

An addressing plan for DREN networks shall be created in collaboration between the Contractor the HPCMPO and its delegates with the allocations according to the plan to be managed by the Contractor with appropriate tools and conventions. The Contractor shall allow for visibility from the HPCMPO into addressing and configurations. The Contractor shall also maintain DNS entries for all addresses upon allocation or implementation. Any new request or requirement for addressing that does not fit the plan shall be coordinated with the HPCMPO or its delegates.

The Contractor shall provide sufficient commodity Internet address space to support the DREN Boundary Zones. The Outreach Internet Service requires the contractor to provide Commodity Internet Addresses. The amount of address space required for IPv4 is a /24 per Internet Transit Service that is ordered. The amount of address space required for IPv6 is a single /48. These must be routed to the Internet, in a single ASN provided by the contractor. Further, the Contractor shall make available these non-associated, non-attributable, prefixes and ASN(s) from one or more tier 1 Internet Service Providers to support functions of DREN and its customers that are appropriately advertised and utilized without Government identification.

6.13.10. Subtask 10. Routing.

The Government may specify interior path selection criteria, propagation of communities of routes within an IP network, prefix advertisement and reception rules at exterior exchanges, and gateway selection criteria for external prefixes learned via peering. The Contractor shall dynamically implement these parameters utilizing appropriate routing protocols and configurations. Examples of routing information exchange parameters include: announcing customer prefixes only within DREN; site routes announced to all external peers including the Internet; and propagating communities of prefixes to customers using BGP community attributes.

6.13.11. Subtask 11. Autonomous System Numbers.

The DREN IP service shall operate as one or more independent and autonomous routing domain(s), independent of all other external networks. Network routing information shall be exchanged with networks external to DREN using BGP4, presented to peers using a Government-owned autonomous system number (ASN) provided to identify the DREN network.

DREN customers may use their own ASN for route exchange with DREN. This information shall be preserved in the AS Path, as it appears to external peers.

6.13.12. Subtask 12. Customer Routing.

Sites shall have the option of announcing their own DoD Network Information Center-(NIC) registered network prefixes to DREN at the SDP interface using BGP4 or static routing. In the case of static routing, the site network routes shall be sourced with the DREN ASN. In the case of BGP, the Contractor shall provide the DREN customer the ability to receive communities of routes (e.g. DREN-

only, DoD-only, Internet, etc). The Contractor shall put in place measures so customers cannot advertise or change advertised prefixes without consent from the HPCMPO.

6.13.13. Subtask 13. IP Multicast.

The Contractor shall provide a robust native IPv6 and IPv4 multicast service both within the DREN community and between DREN and external networks. The service shall include multicast route, source, traffic exchange, and efficient tree management. The service shall meet the same bandwidth and latency requirements as IP Unicast service. The service shall support at a minimum Any Source Multicast (ASM), Source Specific Multicast (SSM), Protocol Independent Multicast - Sparse-Mode (PIM-SM), MSDP (Multicast Source Discovery Protocol), Internet Group Management Protocol (IGMP) v3, and Multicast Listener Discovery (MLD) v2. The infrastructure to support multicast shall be described to show how efficient bifurcation preferably away from the site would occur. In addition the rendezvous point topology should be clearly defined showing how an Anycast Rendezvous Point (RP) structure will be provided. The services shall support security mechanisms as appropriate based on best current practices for the service and shall include the ability to place blocks at external peerings, internal peerings, or customer interfaces including Border Bootstrap Router (BSR) limit, PIM block, and scoping limits by direction of the DREN PM or designate.

6.14. Task 14. Optical Services.

An SDP supporting Optical Services shall allow access to advanced optical layer transport and services and includes Optical Wavelength Service (OWS), other OTU/GFP transport, and Lambda transport. Initially only a small number of SDPs at the higher performance sites are expected to use these services. Optical services SDPs would have bandwidths of OTU1 and greater.

The intention of the optical services family is to allow the interconnection of advanced communication devices, including but not limited to: Government owned DWDM and/or ROADM devices, advanced network encryptors, OTN interfaces in routers which have their own tunable lasers, and OTN transport of other than SONET and Ethernet frames which may want direct access to GFP (e.g. digital video over GFP-T). Some of these advanced communication devices are experimental and would be used to do optical transport experiments over the DREN III optical service.

Optical service shall support connectivity to other external optical networks and optical exchange points. Examples include Regional Optical Networks (RONs), National Lambda Rail's (NLR) WaveNet, and exchange points operated by the Global Lambda Integrated Facility (GLIF). Connections between like-enabled Optical Services SDPs shall be made via service requests and be reconfigurable according to current customer needs. Optical services transmitted into a network SDP through an optical interface shall be routed by the most optimal path over the network to other SDPs supporting optical services. An optical services family SDP shall provide the flexibility to provision multiple OWS, OTU/GFP transport, or Lambda Transport services over a single SDP access circuit.

6.15. Task 15. Evolution of Existing Services.

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

The Contractor shall ensure services provided under this contract remain compatible with current state-of-the-art versions of the applicable standards.

6.15.1. Subtask 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 (TIP) 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.

6.15.2. Subtask 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. It is also expected that the Contractor shall continue to upgrade their underlying core infrastructures at no cost to the Government. For upgrades that constitute new technology insertions, the Contractor shall submit proposals that 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.

The Contractor shall perform regression testing on all major code upgrades to the DREN to ensure features in a previous code release are supported in the new code release. The Contractor shall develop a regression test plan and provide subsequent testing results for any proposed major code upgrade on the DREN for review and concurrence by the Government. Additionally, the Contractor shall provide a final operational test plan and deployment schedule for any major code upgrade for review and concurrence by the Government.

6.15.3. Subtask 3. Technical Refresh and Life Cycle Engineering Support.

A fundamental element of the success of the DREN environment is the ability to implement and support leading edge and next-generation network capabilities that grow and evolve with the needs of the community that in turn is creating next-generation solutions for the DoD. In pursuit of this underpinning goal, the Contractor shall provide a coherent approach to sustainment, robustness, and advancement for the life of the DREN network architecture and services. This may include but not be limited to architectural planning, life cycle engineering, or equipment technical refresh in order to support the current and TIP-initiated services and features of the DREN.

6.15.4. Subtask 4. Government versus Contractor Initiated Proposals.

6.15.4.1. Element 1. Government Initiated.

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

6.15.4.2. Element 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.

6.16. Task 16. Contractor Simulation Environments and Test Labs.

DREN is designed to be a leading edge production environment and as such, simulation and test lab capabilities can impact strategic direction and implementations in significant ways. The Contractor shall make simulation environments and test labs available as needed for Contractor's engineering / operations to simulate or test various aspects of the DREN. As part of the process of implementing new features, systems, or protocols on the DREN, the Contractor shall enable access by the HPCMPO for visibility, interaction, and possible control of emulation environments where engineering, simulation,

and pre-implementation testing are performed. Use of these environments shall also be used where feasible on routine configuration and route changes to minimize unexpected impacts in time or performance to the operational environment.

6.17. Task 17. 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 paragraph 12 Security). Requirements for each of these Network Management functions are defined below.

6.17.1. Subtask 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 HPCMPO 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.

Network management and supervision systems must operate over an IPv6 infrastructure when communicating with network elements and support systems.

6.17.2. Subtask 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.

6.17.2.1. Element 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.

6.17.2.2. Element 2. Problem and Fault Isolation – Ethernet Services.

In most cases, the Government will verify performance at layer 2 and below by running IP based tests over those layers. If these tests do not perform well, then problem isolation below the IP layer may be required. Each SDP shall have the ability to loopback to a layer 2 VLAN as requested to aid in network testing. The Contractor shall support these standards and industry best practices in this area.

6.17.2.3. Element 3. Problem and Fault Isolation – Internet Protocol Service.

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:

- e. Demonstrating end-system (directly attached CPE) performance.
- f. Reporting end-system (directly attached CPE) performance failures.
- g. Detecting and resolving physical layer and physical media failures.
- h. Detecting and resolving media access protocol failures.
- i. 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 misconfigured routing tables, and defective or misconfigured routing policies.
- j. Demonstrating interoperability with all SDPs that are required to support IPv4 and IPv6.

6.17.2.4. Element 4. Problem and Fault Isolation – Optical Services.

The Contractor shall provide unambiguous analysis of service failures at the optical SDPs through fault detection and isolation capabilities, and enable service restoration at the optical 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. In most cases, the Government will verify performance at the optical layer by running IP based tests over that layer. If these tests do not perform well, then problem isolation at the optical layer may be required¹. The Contractor shall follow best industry practices in this area.

6.17.2.5. Element 5. Problem and Fault Isolation – SDP Utilized as Gateways.

The Contractor shall monitor health and connectivity to all external networks at all external exchange points. The Contractor shall resolve problems with the network management organizations of the other networks. The Contractor shall keep logs of all the problems and corrective actions taken to resolve the problems at these locations.

6.18. Task 18. 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.

6.18.1. Subtask 1. Performance Measurement and Validation.

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, quantify and report the following:

- a. Sustained and maximum IP output transfer rate at the SDP; and each customer facing interface.
- b. Sustained and maximum IP input transfer rate at the SDP, and each customer facing interface.

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

¹ G.709 defines Operations, Administration, Maintenance, and Provisioning (OAM&P) capabilities at the optical layer.

6.19. Task 19. Configuration Management.

Configuration Management is the process that preserves the integrity of the network configuration. The DREN Configuration Control Board (CCB) will represent Government interests in weekly status meetings with the Contractor. The CCB will review proposed implementation changes and schedules. All Configuration Management records shall be kept current, accurate, and maintained for the duration of the contract.

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

- a. IPv4 and IPv6 subnet structure, routing table configurations;
- b. Multicast configurations
- c. Network management and external access control list and/or firewall configurations;
- d. Network device (Core and SDP) configurations in general;
- e. Circuit / trunk number;
- f. State of the network elements (such as in service, out of service for routine or diagnostic test, disconnected, new, etc.);
- g. Inventory of ports and services at each SDP including customer access and network access;
- h. Any other equipment installed by the Contractor to provide service such as, network management and monitoring, network operations center / help desk information systems, power, rectifiers, UPS, HVAC, etc.; and
- i. 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.

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

Configuration information of relevance to individual DREN customers shall be available to those customers only.

The Contractor shall document configuration management meeting minutes in an electronic format that is accessible to HPCMPO personnel via a web-based application.

6.20. Task 20. Network Management Reporting.

Report monitoring for 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 DREN 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 shall propose formats for generated reports for Government approval.

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 the SDP Service Availability subtask.
- b. Service degradation time – the time when there is a severe deterioration in performance of the network.
- c. 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:

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.

- d. 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:

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.

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.

6.21. Task 21. Network Visibility and Customer Tools Sets.

See **Section 6.23 Task 23. Customer Care.**

6.22. Task 22. Domain Name Service.

The Contractor shall be authoritative for the DREN.NET domain in a Master (Contractor system/s)-Slave (Government systems) configuration utilizing DNSSEC where possible. The Contractor shall ensure all IP addresses associated with the DREN.NET domain (to include all IPv4 and IPv6 addresses utilized on all Contractor and Government supplied hardware that comprise the DREN and its support systems) are continually registered in the domain.

6.23. Task 23. Customer Care.

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

- a. Provisioning and tracking of service requests and delivery orders;
- b. Reporting and tracking of DREN problems;
- c. Monitoring of Contractor's performance;
- d. Accounting management;
- e. Obtaining customer support and instructional services and,
- f. Provisioning network configuration, utilization and performance monitoring tools.

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 subparagraphs outline the Contractor's responsibilities pertaining to service provisioning, service and problem management, reporting, accounting management, and customer support services.

6.23.1. Subtask 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 the particular Delivery Order and this PWS. Service shall be provisioned through Service Requests and Delivery Orders. The Contractor shall process delivery orders as directed by the Contracting Officer.

6.23.1.1. Element 1. Service Requests and Delivery Orders.

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

6.23.1.1.1. Subelement 1. Service Requests.

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

6.23.1.1.2. Subelement 2. Delivery Orders.

The Delivery Order (DO) includes requests for activities that are not performed by the O&M staff as a day-to-day operation. The DOs will be initiated by the Contracting Officer (CO) to the Contractor. The Contractor shall only process delivery orders issued by the CO or other designated authorized representative.

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

6.23.2. Subtask 2. Provisioning of Service Requests and Delivery Orders.

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

6.23.2.1. Element 1. Provisioning of Service Requests.

The following delivery intervals depicted in Table 6.23.2a are required for service requests. Service requests shall include but are not limited to route modification; new or modified VLAN; firewall modification; customer interface activation or modification; and new, modified, or updated DNS entries managed by the DREN NOC.

Table 6.23.2a Required Delivery Intervals

Service	Standard
Routine Service Request	24 hours
Priority Service Request	4 hours

The Contractor shall provision service requests on a priority basis upon specific request by the DREN PM or designates.

6.23.2.2. Element 2. Provisioning of Delivery Orders.

Unless otherwise required by a DO, the Contractor shall develop appropriate plans and provision services in accordance with the requirements in the Implementation and Transaction Actions and the subtask (Subtask 6.23.1). The following delivery intervals depicted in Table 6.23.2b are required for DOs.

Table 6.23.2b Required Provisioning Intervals for Delivery 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 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.

6.23.2.3. Element 3. Expedited Delivery 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 DO may be in the form of electronic mail, fax, telephone call, or verbal request to be followed by a written DO. A written DO will be issued confirming any verbal request. Service provisioning times will be negotiated for each Expedited DO 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 DO does not relieve the Contractor of the responsibility to perform.

6.23.2.4. Element 4. Service Request and Delivery Order Tracking.

The Contractor shall enter all service requests and DOs in its Customer Service Management system, described in and use it to track progress of the request from origination to completion including escalations when they occur. At a minimum, the Contractor shall maintain record of the following for each Service Request / DO and submit an example of a proposed tracking record

- 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. Critical path for activities required for order completion;
- f. SDP location (actual address of physical location as well as the NPA/NXX of the location);
- g. Service / agency name;
- h. Account code;
- i. Due date;
- j. Primary and alternate DREN contact name, address, email, fax, cell number (if provided) and telephone number;
- k. Order status report; and
- l. Non-recurring and recurring costs associated with DO.

The provisioning data shall be available to the High Performance Computing Modernization Program Office (HPCMPO) and the customer SDP on a web-based real-time automated basis to allow Government tracking of routine operations or Government-initiated delivery 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 6.23.2c. These reports can be delivered either electronically via email or be made available through a web-based interface.

Table 6.23.2c 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	$\frac{\text{Cumulative time to respond to all related Service Requests completed}}{\text{Number of Service Requests completed}}$
Mean time to provision SDP service orders by type of service orders	$\frac{\text{Cumulative time to respond to all related Service Requests completed}}{\text{Number of Service Requests completed}}$

6.24. Task 24. 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, help desk standard operating procedures, problem management and escalation procedures, as well as a record keeping system.

6.24.1. Subtask 1. Help Desk / Network Operations Center.

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 and capable of accepting and processing the report. In addition, the Contractor shall accept Secure Socket Layer (SSL) web-based or digitally signed e-mail service requests and trouble reports also on the 7 x 24 basis. Calls may come from the HPCMPO or the customers served at the SDP sites. Trouble tickets that result in configuration changes to the WAN will only be implemented if approved by the HPCMPO. 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. Where multiple trouble tickets are opened on a related issue, a methodology for grouping tickets under a parent – child tracker shall be implemented. The Contractor shall propose a TT format and record keeping system for Government approval.

To ensure consistent and professional customer support is provided, the Contractor shall develop Standard Operating Procedures that address the following issues:

- a. Network Management Tool Alarms;
- b. Trouble Ticket Priorities;
- c. Trouble Ticket Response Times;

- d. Customer-Initiated Trouble Tickets;
- e. Required Information in Trouble Tickets;
- f. Trouble Ticket Escalation Procedures;
- g. Special Handling Tickets;
- h. Change Request Tickets;
- i. Domain Name Service;
- j. DREN NOC and Network Security Incident Tickets;
- k. Outage Reporting and updates for Priority One, Two Three and Four Issues;
- l. Maintenance Notifications, urgent, standard notification routines;
- m. Rescheduling of Normal or Routine Maintenance Categories;
- n. Updates to Maintenance Notifications;
- o. Critical or Emergency Maintenance Notifications;
- p. Post-Maintenance and Follow-Up;
- q. Shift Turnover;
- r. Customer Support Etiquette;
- s. Telephone Communications; and
- t. Electronic Communications (Email, Video, Instant Messaging)

6.24.1.1. Element 1. Customer Problem Management.

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

6.24.1.2. Element 2. 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 HPCMPO;
- 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 6.24.1a.

Table 6.24.1a Required Response and Repair Times

Category	Time Interval
Time to answer trouble report by human operator	60 seconds
Time to respond to a web based trouble report	30 minutes
Time to respond to an email trouble report	1 hour
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 HPCMPO*	4 hours
• Non-Key SDP sites designated by HPCMPO	12 hours
• Internet / Peering location	4 hours
Time to repair with on-site field visit:	
Attachment A Key SDP sites designated by HPCMPO*	5 hours
1. Non-Key SDP sites designated by HPCMPO	13 hours
a. Internet / Peering location	25 hours

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

6.24.1.3. Element 3. 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 HPCMPO and the designated customer site POCs 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. The list of personnel shall contain at least contact information (email, phone, fax, mailing address, and cell number if provided) for the following:

- a. Primary and Alternate POCs;
- b. After hours POC;
- c. Security Manager;
- d. Designated Approving Authority; and
- e. Other POCs as specified by the customer via DREN Service Agreement documentation.

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.

6.24.2. Subtask 2. 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. Description of how service was verified as working.
- l. Date and time of closure of the TT.
- m. Data relating to problem escalation required in Element 6.24.1.3.

The data in the trouble ticket shall be available on a web-based real-time automated basis to the HPCMPO, 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 HPCMPO to match the Contractor's trouble ticket number, including changes or bundling of tickets and escalations, with the trouble ticket number tracked by the HPCMPO.

6.25. Task 25. 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 HPCMPO;
- b. Provide an on-line database of trouble events available to HPCMPO 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;
- c. Provide an on-line report generation capability that allows HPCMPO 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 Customer Care Problem Resolution Table.
- d. Provide a near real time on-line report of core and customer IP address allocations that is available to HPCMPO personnel;
- e. Provide a near real time on-line report of network management IP address allocations that is available to HPCMPO personnel;
- f. Provide a near real time, on-line DREN intra-connectivity status available to HPCMPO personnel only;
- g. Provide a near real time on-line report of core and customer VLAN allocations that is available to HPCMPO personnel;
- h. Provide a near real time on-line report of core and customer C-Band optical allocations that is available to HPCMPO personnel
- i. Documentation on external peers and Core Node, NAP and SDP Plan network diagrams available to HPCMPO personnel only;
- j. Provide on-line, all document deliverables available to HPCMPO personnel only;
- k. Provide on-line, all Delivery Orders available to HPCMPO personnel only;
- l. Provide on-line all Post Accounting reports available to HPCMPO personnel only;
- m. Provide on-line all Service Requests available to HPCMPO personnel only;
- n. Provide on-line Weighted MTTR reports available to HPCMPO personnel only;

- o. Provide on-line reports from interactive network trending tools available to HPCMPO personnel only;
- p. Provide on-line Peak Usage Reports available to HPCMPO personnel only;
- q. Provide Round trip time information available to HPCMPO personnel only;
- r. Provide SLA Reports available to HPCMPO personnel only;
- s. Provide on-line WAN Usage Reports available to HPCMPO personnel only;
- t. Provide on-line all SDPs and customer Interfaces mapped to individual customer route advertisements; and
- u. Provide BGP route reports for various BGP route tables and BGP communities.

Table 6.25a 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	$\frac{\text{Cumulative time to respond to all TTs}}{\text{Total Number of TTs created}}$
Mean time to repair w/o dispatch	$\frac{\text{Total outage time for all TTs w/o dispatch}}{\text{Total number of TTs created}}$
Mean time to visit by field technician — Major sites — Other sites	$\frac{\text{Total time to visit by a field tech for all TTs w/ dispatch}}{\text{Total number of TTs requiring dispatch}}$ Separate report for major and other sites
Mean time to repair with field dispatch — Major sites — Other sites	$\frac{\text{Total outage time for all TTs with dispatch}}{\text{Total number of TTs created}}$ Separate report for major and other sites
Percent of TTs cleared within time intervals specified in Element 6.24.1.2 — Major sites — Other sites	$\frac{\text{TTs cleared within designated time limits} * 100}{\text{Total number of TTs created}}$ Separate report for major and other sites
Total number of TTs	Per trouble desk report
Percent TTs requiring field visit	$\frac{\text{Number TTs requiring dispatch} * 100}{\text{Total number TTs created}}$
Percent TTs escalated by TT type — by level of escalation	$\frac{\text{Number TTs requiring escalation} * 100}{\text{Total number TTs created}}$ Separate report for each level of escalation

Problem Management Performance Parameter	Calculation (All Quantities Measured On A Monthly Basis)
Percent Trouble reports answered within designated time interval <ul style="list-style-type: none"> — initial response — human operator response 	$\frac{\text{Cumulative time to respond to all TTs}}{\text{Total Number of TTs created}}$ Separate report for initial response and human operator response

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

6.26. Task 26. 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 HPCMPO in a user-friendly format with web access.

6.27. Task 27. Customer Support and Instructional Services.

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

6.27.1. Subtask 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. Utilize on-line Customer Care tools;
- d. Request SDP routine operational services; and
- e. Perform 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.

6.27.2. Subtask 2. 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.

6.27.3. Subtask 3. Engineering Studies.

Engineering Studies technical support services shall include in-depth 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.

6.27.4. Subtask 4. Customer Care Tools.

The Contractor shall provide an interactive, protected web-based application that provides a central document repository and an interactive capability for DREN customers. This resource will allow site point of contacts to have visibility into site related documentation, site and network related configuration, trouble ticket status and performance of the network. The Contractor shall work with the Government to establish separation of information between DREN communities of interest when needed.

At a minimum, the Contractor shall provide the following:

- a. A customer generated report capability for real-time reporting tools to include site interface descriptions, status, utilization statistics and SLA performance metrics;
- b. Interactive looking glass tools to include interface commands such as ping, traceroute, and route queries within the DREN community and peering exchange points;
- c. Firewall configuration search tools to query access control lists for ports and protocols and exception filters at peering exchange points and customer SDPs;
- d. SDP device and Core Node device multicast configuration, status and statistical information;
- e. SDP device hardware configuration, routing information and interface utilization statistics;
- f. The ability to input and view site initiated trouble tickets and status, information on routine maintenance and unscheduled outages that are service impacting for one or more sites; and
- g. Enhanced service and Optical Wave Services (OWS) specific tools.

6.28. Task 28. Contract Phase Out.

The Contractor shall perform the contract phase-out activities necessary to support the transition of services to a follow-on provider. All work under this task will be initiated through separate delivery orders. The delivery 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 III to a follow-on provider are described below.

6.28.1. Subtask 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:

6.28.1.1. Element 1. Development of Contract Phase-out Transition Plan.

The Contractor shall coordinate with and assist the follow-on Contractor(s) in establishing the most cost-effective method for transitioning from DREN III Services 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.

6.28.1.2. Element 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;
- c. LEC circuit numbers and carrier; and
- d. As-built diagrams.

6.29. Task 29. 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. The Contractor shall provide bridging gateway(s) and bridging gateway support in accordance with the phase out transition plan.

7. PERFORMANCE STANDARDS:

Performance Standard	Acceptable Quality Level	Method of Surveillance	Deliverable #
6.1.4 Subtask 4. Progress Reporting.	Performance is based on the effectiveness of transition and progress report items. Issues are resolved in a satisfactory and timely manner.	Routine review of reports to verify items are tracked and resolved. Review Quarterly Progress Reports.	1
6.1.5 Subtask 5. Support for the DREN Configuration Control Board (CCB).	CCB meetings will be conducted. All agenda items are tracked weekly by the Contractor and resolved on a satisfactory basis in a timely manner. Action items that are not resolved will be escalated.	Routine review of weekly meeting minutes to verify that agenda items are tracked and resolved as appropriate. Review Weekly CCB minutes.	2

Performance Standard	Acceptable Quality Level	Method of Surveillance	Deliverable #
6.1.6 Subtask 6. DREN Technical Advisory Panel.	Performance occurs with the planning and execution of the DREN TAP meeting and successful completion of assigned tasks	Review of DREN TAP meeting agenda and minutes	3
6.1.7 Subtask 7. Operational and Management Review.	Actions items are tracked quarterly and resolved in a satisfactory and timely manner.	Routine review of quarterly meeting minutes to verify that agenda items are tracked and resolved. Review Project Management Review.	4
6.1.8 Subtask 8. Annual Planning and Design Review.	Performance occurs with adequate planning for technology enhancements, network trends and equipment refresh.	Review of Annual Planning and Design Review.	5
6.1.9 Subtask 9. Annual DREN Networking and Security Conference.	Performance occurs with the planning and execution of the annual DREN conference.	Review of Annual DREN Networkers Conference.	6
6.2 Task 2. Implementation and Transition.	Plans are accepted on-time with only minor revisions required.	Review of Updated Draft IPC Plan, Final IPC Plan, Draft Comprehensive Implementation and Transition Plan, Final Comprehensive Implementation and Transition Plan, Draft Master SDP Plan, and Final Master SDP Plan.	7,8,10, 11,12, 13,
6.3 Task 3. Implementation and Transition Actions.	Performance is based on the successful execution of the IPC Demonstration.	Review IPC Demonstration Report, SDP Site Surveys, and Individual SDP Report.	9,14,15

Performance Standard	Acceptable Quality Level	Method of Surveillance	Deliverable #
6.3.3 Subtask 3. Transition Review.	Performance is based on the effectiveness of transition.	Review of monthly reports and weekly meeting minutes.	1,2
6.4.1 Subtask 1. Individual SDP Reports.	As-build drawings accurately reflect the actual configuration of the installed SDP. All variations from the Master SDP Plan are identified. Acceptance test report includes all pertinent data regarding test results	Review of Individual SDP Reports	15
6.4.2 Subtask 2. Acceptance Test Plan.	Acceptance test is developed and executed with problems resolved in a satisfactory manner.	Review of Acceptance Test Plan component of the CITP and Master SDP Plan; Review of Individual SDP Reports.	10,11, 12,13, 15
6.4.3 Subtask 3. SDP Modification.	Reports are delivered on-time and executed with problems resolved in a satisfactory manner.	Review of proposed modifications.	14, 15
6.4.5 Subtask 5. Termination / Restoration.	Reports are delivered on-time and executed with problems resolved in a satisfactory manner.	Review of proposed actions.	14, 15
6.5 Task 5. Install, Modify, Terminate, and Restore Gateway Functions.	Performance based on effectiveness of network peers and gateway services.	Routine inspection of deliverable products and services.	N/A
6.6 Task 6. Disaster Recovery and Contingency.	Performance based on continuity of service delivery.	Routine inspection of deliverable products and services.	N/A

Performance Standard	Acceptable Quality Level	Method of Surveillance	Deliverable #
6.7 Task 7. Data Transfer Requirements.	Performance based on the quality of services delivered.	Routine inspection of deliverable products and services.	N/A
6.8 Task 8. SDP Characteristics.	SDP Data transfer rates for peak and sustained rates are defined in Table 6.8.3a.	Routine performance measurement and validation as described in Subtask 6.18.1.	N/A
6.9 Task 9. SDP Functional Requirements. 6.9.1 Subtask 1. SDP and Service Availability Requirements.	SDP and Service Availability Requirements are defined in Subtask 6.9.1. Each active SDP shall experience no more than 30 minutes of outage per month.	Routine method for performance evaluation as described in Task 6.18 will be evaluated based on routine review of network availability. Billing credits will be applied for outages exceeding limits described in Table 6.9.1a.	16
6.9.2 Subtask 2. Network Performance: Packet Loss.	The loss of IP packets submitted to the network shall not exceed 0.1% at any time.	Routine performance evaluation based on review of packet loss data.	17
6.9.3 Subtask 3. Network Performance: Latency.	Maximum roundtrip time in milliseconds (latency) for traffic over similar services deployed at two SDPs shall not exceed $(.02 * \text{Inter-SDP distance in kilometers}) + 20$	Routine performance evaluation based on review of IP Latency data. At a minimum to consist of ICMP ping messages generated and measured at all networked SDPs once per minute, 24 hours per day year round and report results.	18
6.9.4 Subtask 4. Network Performance: Availability	Network Availability Requirements are defined in Subtask 6.9.4. The aggregate up time of all active SDPs shall be such that Network Availability meets a minimum of 0.999 (99.9%) for each calendar month.	Routine method for performance evaluation as described in Task 6.18 will be evaluated based on routine review of network availability. Billing credits will be applied for total outages exceeding limits described in Table 6.9.4a.	16

Performance Standard	Acceptable Quality Level	Method of Surveillance	Deliverable #
6.10 Task 10. Contractor Verification of Services.	Contractor services are successfully delivered and demonstrated to operate as designed.	Review Individual SDP Report and Aggregate SDP Test Plan and Aggregate SDP Report.	15,19, 20
6.12 Task 12. Ethernet and VLAN Services.	Services conform to requirements identified in PWS.	Routine inspection of deliverable products and services.	N/A
6.13 Task 13. Internet Protocol Service.	Services conform to requirements identified in PWS.	Routine inspection of deliverable products and services.	N/A
6.14 Task 14. Optical Services.	Services conform to requirements identified in PWS.	Routine inspection of deliverable products and services.	N/A
6.15 Task 15. Evolution of Existing Services.	Contractor services evolve to incorporate commercially available new enhancements over the life of the contract.	Review of Technology Insertion Proposals.	N/A
6.17 Task 17. Network Management.	The network is monitored for fault management 24 hours a day, 7 days a week (7x24). Problems are identified, isolated and resolved within a timely manner.	Routine review of trouble tickets. Review of Performance Management Data and Network Management Reporting data.	21, 22
6.23 Task 23. Customer Care.	Service requests and Delivery Orders are completed accurately and in a timely manner (see Table 6.23.2a and Table 6.23.2b).	Routine review of Delivery Order tracking data and Service Provisioning Performance Report data.	23, 24

Performance Standard	Acceptable Quality Level	Method of Surveillance	Deliverable #
6.24 Task 24. Service and Problem Management.	The Help Desk / Networks Operations Center is responsive. Trouble reports are resolved in a satisfactory manner. Response and repair times are identified in Table 6.24.1a.	Routine review of Help Desk / Trouble ticket data as described in Task 6.24.1.	25
6.25 Task 25. Customer Care Data and Reports.	Problems are resolved in a timely and satisfactory manner (Table 6.25a)	Routine review of Customer Care Problem Resolution Data Reports.	26
6.26 Task 26. Accounting Management.	DREN quality of service, costs and credits are maintained.	Routine review of Accounting Management Data.	27
6.27 Task 27. Customer Support and Instructional Services.	Adequate training and online customer support tools are provided.	Review of Instructional Services Training and Technical, Telecommunications Support / Engineering Studies and Customer Care Tools.	28, 29, 30
6.28 Task 28. Contract Phase Out.	Adequate planning and documentation is provided for transition.	Review of Contract Phase-Out Transition Plan.	31
6.2.2.3 Element 3. Security. & 12 Security.	Adequate documentation, plans, and procedures are in place and executed.	Routine inspection of deliverables.	10, 11, 32, 33, 34
12.10 Certification and Accreditation (C&A) support.	Security accreditation packages are submitted on time and executed with problems resolved in a satisfactory manner. Packages are maintained / updated when network configuration changes.	Periodic review of DIACAP package.	35, 36

Performance Standard	Acceptable Quality Level	Method of Surveillance	Deliverable #
12.13.4 Security Incident Reporting.	Monthly security reports submitted in a timely manner. Incidents handled IAW HPC CERT.	Routine review of monthly reports.	37, 38, 39
12.13.5 Security Vulnerabilities.	Security vulnerabilities addressed IAW DOD IAVA process, including reporting / mitigation dates.	Review of IAVA reports as required.	N/A
12.13.6 Security Audit Reporting.	Audit records shall be maintained in a manner consistent with 12.13.6.	Periodic review of on- and off-line logs.	40
12.13.7 Continuity of Operations.	Plans and procedures will be submitted in a timely manner.	Review of plan and test results as they are generated.	41

8. INCENTIVES.

Billing credits will be applied for failure to meet performance standards as identified in this PWS.

9. PLACE OF PERFORMANCE.

This work will be performed at Contractor facilities, customer sites, Government sites and peering locations as designated in the delivery orders.

10. PERIOD OF PERFORMANCE.

120 months after contract award including a 36-month base period and seven 12-month option periods.

11. DELIVERY SCHEDULE

Deliverable #	Deliverable Title	Format	Due Date and Frequency	Distribution / Copies	PWS Ref #
1.	Monthly / Quarterly Progress Report	Online	Monthly on the 15 th through IPC– Quarterly after IPC - 15 th of the month	Program Office COR Contracting Office Available online specified users	6.1.4, 6.3.3
2.	Configuration Control Board	Online	Weekly	Available online specified users	6.1.5
3.	DREN Technical Advisory Panel	Online	Quarterly and as needed	Program Office COR Contracting Office Available online specified users	6.1.6
4.	Operation and Management Review	Online	Quarterly – 15 th of the month	Program Office COR Contracting Office Available online specified users	6.1.7
5.	Annual Planning and Design Review	Online	Yearly	Program Office COR Contracting Office	6.1.8
6.	Annual DREN Networking and Security Conference	Online Registration & Materials	Yearly	Program Office COR	6.1.9
7.	Draft IPC Plan	Online	30 Calendar days after contract award	Program Office COR Available online designated users	6.2.1

Deliverable #	Deliverable Title	Format	Due Date and Frequency	Distribution / Copies	PWS Ref #
8.	Final IPC Plan	Online	15 Calendar days after receipt of comments on Draft from the Government	Program Office COR Available online designated users	6.2.1
9.	IPC Demonstration Report	Online	30 Calendar days after completion of IPC Tests	Program Office COR Available online designated users	6.3.1
10.	Draft Comprehensive Implementation and Transition Plan	Online	30 Calendar days after acceptance by the Government of IPC Test Report	Program Office COR Available online designated users	6.2.2
11.	Final Comprehensive Implementation and Transition Plan	Online	30 Calendar days after receipt of comments on Draft CITP from the Government	Program Office COR Available online designated users	6.2.2
12.	Draft Master SDP Plan	Online	30 Calendar days after Final IPC Plan acceptance by the Government	Program Office Site Representative Available online designated users	6.2.2.8
13.	Final Master SDP Plan	Online	15 Calendar days after receipt of comments on Draft from the Government	Program Office Site Representative Available online designated users	6.2.2.8
14.	SDP Site Surveys	Online	30 Calendar days after receipt of order	Program Office Site Representative Available online designated users	6.2.2.7

Deliverable #	Deliverable Title	Format	Due Date and Frequency	Distribution / Copies	PWS Ref #
15.	Individual SDP Reports	Online	15 Calendar days after completion of SDP Acceptance Test	Program Office Site Representative COR Available online designated users	6.4.1
16.	Network Availability	Online	Monthly – 10 th of every month	Available on-line designated users	6.9.1, 6.9.4
17.	Packet Loss	Online	Daily	Available on-line designated users	6.9.2
18.	IP Latency	Online	Daily	Available on-line designated users	6.9.3
19.	Aggregate SDP Test Plan (non-IPC)	Online	30 calendar days after order received from Government	Program Office COR Available online designated users	6.10.2
20.	Aggregate SDP Test Report (non-IPC)	Online	15 calendar days after test completion	Program Office COR Available online designated users	6.10.2
21.	Performance Management Data	Online	As Required	Program Office COR Available online designated users	6.18.1
22.	Network Management Reporting	Online	Real Time	Available on-line to designated users	6.20
23.	Service Request and Delivery Order tracking data	Online	Real Time	Available on-line to designated users	6.23.1.1

Deliverable #	Deliverable Title	Format	Due Date and Frequency	Distribution / Copies	PWS Ref #
24.	Service Provisioning Performance Report	Online	Monthly – 15 th of every month	Program Office COR Available online designated users	6.23.2.4
25.	Help Desk / Trouble ticket data	Online	Real Time	Available on-line to designated users	6.24.1
26.	Customer Care Data Reports	Online	Real Time	Available on-line to designated users	6.25
27.	Accounting Management Data	Online	Update monthly	Program Office COR Available on-line to designated users	6.26
28.	Instructional Services Training	Online	As proposed by the Contractor	Program Office DREN Managers and Users	6.27.1
29.	Technical and Telecommunication Support / Engineering Studies	Online	As Requested	Program Office COR Available online designated users	6.27.2, 6.27.3
30.	Customer Care Tools	Online	Hourly	Designated Users	6.27.4
31.	Contract Phase-Out Transition Plan	Online	30 calendar days after receipt of order	Program Office COR Available online designated users	6.28.1.1
32.	Action taken on results of Security Tests / Assessments	Online	15 calendar days after team brief-out	Program Office COR	12.10

Deliverable #	Deliverable Title	Format	Due Date and Frequency	Distribution / Copies	PWS Ref #
33.	Security Operations Plans	Online	60 calendar days after award - Updated Annually	Program Office COR	12.10(e)
34.	Standard Operating Procedures	Online	60 calendar days after award - Updated Annually	Program Office COR	12.10(f)
35.	DIACAP Package	Online	60 calendar days after receipt of first delivery order and updated continually	Program Office COR	12.11
36.	Security Test and Evaluation Plan	Online	60 Calendar days after contract award and updated annually	Program Office COR	12.12
37.	Incident Reporting Plan and Procedures	Online	30 calendar days after SOP acceptance – Updated Annually	Program Office COR	12.13.4
38.	Incident Plan and Procedures Report	Online	Monthly – 15 th of every month	Program Office COR	12.13.4
39.	Security Incident Reporting	Online	Immediate upon detection	Program Office COR	12.13.4
40.	Security Audit Reporting Data	Online	Updated Daily	Available on-line designated users	12.13.6
41.	Computer / System Emergency Response Plan and Procedures	Online	60 calendar days after award - Updated Annually	Available on-line designated users	12.13.7
42.	Other Conferences	Online Registration & Materials	Yearly	Program Office COR	6.1.10

Deliverable #	Deliverable Title	Format	Due Date and Frequency	Distribution / Copies	PWS Ref #
---------------	-------------------	--------	------------------------	-----------------------	-----------

**Standard Distribution: 1 copy of the transmittal letter without the deliverable to the Contracting Officer; 1 copy of the transmittal letter with the deliverable to the Primary COR or TM*

All deliverable materials and documents under this PWS shall be considered the property of the Government. All materials and documents provided online shall be available for download and use by the Government at no additional cost.

12. SECURITY.

Work to be performed under this PWS will be of up to and including the secret level as outlined in the following sections as well as the current DD254 Department Of Defense Contract Security Classification Specification associated with this contract. All personnel associated with this contract, shall have sufficient background investigations or clearances according to the standards set in DoD Instruction 8500.2 and DoD 5200.2-R and indicated in the DD254. Contractor shall submit request for visit authorization in accordance with DoD 5220.22M (Industrial Security Manual) no later than one week prior to visit. Requests shall be forwarded via the DoD facilities Security Office to Attn: Security Office for certification of need to know by the specified TCOR. Security Training shall be provided. Contractor personnel shall be appropriately trained and certified prior to being engaged. The Contractor shall also provide the requested mix of labor categories pertaining to applicable tasks as directed by the PCO or Delivery Order in support of training requirements. Contractor personnel not certified within 6 months of assignment or who fails to maintain their certified status will not be permitted to carry out the responsibilities of the position, and shall be replaced with personnel that meet the minimum certification requirements as mandated above.

12.1. Organization.

In addition to meeting the security requirements in contract clause the Contractor shall establish an operational security (OPSEC) program in strict compliance with the National Industrial Security Program Operating Manual (DoD 5220.22-M) and related security directives.

12.1.1. Facility Clearance.

The Contractor shall be fully prepared to submit the appropriate documentation and information at the time of contract award to establish a SECRET facility clearance for the DREN Network Operations Center (D-NOC) as directed in DD254.

12.1.2. Personnel.

The Contractor shall conform to the provisions of DoD 5220.22M, the Privacy Act of 1974, and related instructions. The Contractor shall employ personnel who possess and can maintain appropriate background investigations and security clearances as detailed in DD254. Cost to meet these security requirements is not directly chargeable to a delivery order.

12.1.3. Control of Contractor Personnel.

The Contractor shall comply with site security regulations. All persons engaged in work while on Government and Government-leased property shall be subject to inspection of their vehicles at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location. Contractor Personnel located within Government spaces shall be subject to Identification and badge requirements (Contractor Picture Badge) for Contractor Identification.

Contractor personnel directly supporting the Contract shall be required to obtain a Common Access Card (CAC) with PKI for access to Department of Defense facilities and websites. In addition, a hardware solution to securely read the card via a personal computer (PC), and approved software for reading the CAC (ex. ActiveGold) is required. Security requirements are integral to the successful accomplishment of delivery orders under the contract.

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 HPCMP in protecting DREN from threats both internal and external. The Contractor shall validate that the hardware and software comply with DoD security requirements specified in this PWS and DD254.

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 PWS. 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 8500.1 and DoD Instructions 8500.2 and 8510.01.

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 PWS. The Contractor shall incorporate the security requirements and features described in this PWS into the configuration, implementation, and operation of a DREN 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.

12.2. DREN Security Requirements.

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 profiles and traffic. DREN shall satisfy security requirements described in: DoD Directive 8500.1 and DoD Instructions 8500.2 and 8510.01. 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 subparagraphs: Access Control, Identification and Authentication, Confidentiality and Integrity, Physical Security, and Personnel Security.

12.3. 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 PWS. 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:
- e. 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
- f. Require those operations personnel to be authenticated before allowing an operator session.

12.4. Non-Contractor Network Resource Access.

At the request of the Government, the Contractor shall provide HPCMP personnel read-only access and Simple Network Management Protocol (SNMP) read access to networking resources for the purpose of reviewing hardware configuration information and obtaining statistical information.

12.5. 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 and control attributes for all operations personnel authorized to access the system. As a minimum, the following attributes belonging to each individual operations personnel shall be controlled: 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 140-2), 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:

- d. 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);Trusted centralized authentication server to authenticate a third party operator.

12.6. 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 DoD Directive 8500.1. 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 Internet Exchange points and 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 and ;
- b. Have the ability to detect modification of sensitive management / control data transmitted between network management facilities and network components during transmission.

12.7. 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 DoD Directive 8500.1, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; and DoD 5200.8-R, Physical Security Program.

12.8. Personnel Security.

The Contractor shall ensure compliance with all DoD Personnel Security Requirements for access to Controlled, Unclassified Information (CUI). The Contractor shall provide personnel security in accordance with DoD 5200.2-R, Personnel Security Program, and DoD Instruction 8500.2, Information Assurance Implementation. The Contractor shall ensure that all Contractor personnel have the necessary Government background investigations for IT-I and IT-II designation prior to accessing the DREN network resources. The Contractor shall not claim lack of an appropriate investigation as a reason for noncompliance.

12.9. Security Enhancing Network Features.

At the direction of the Government, the Contractor shall provide the following enhanced capabilities on any specified path in the network:

- a. Unicast Reverse Path Forwarding (URPF): In order to limit the appearance of spoofed addresses on the network source IPs should be verified for accuracy. URPF shall be used on all customer facing interfaces to accomplish this protection.
- b. BOGON and Martian filtering: Because they have no legitimate use, BOGON filtering shall be applied at all edges of the network. Martian filtering shall also be utilized to restrict forwarding invalid packets. The Contractor should describe the location and techniques to accomplish this requirement.
- c. Remote Triggering Black Hole (RTBH): Traffic stream adjustments will be required for packets requiring some additional handling. The Contractor shall implement RTBH to support traffic sink, scrub, and redirection.
- d. Sink: Traffic identified as malicious traffic by the Government will be sent to a designated dead end monitoring devices managed by HPCMP.
- e. Scrub: Traffic of a questionable nature or of particular interest to the Government shall be routed to device(s) managed by the HPCMP to perform inspection. This traffic will then either be passed unaffected, repaired, filtered, or blocked. The resulting packets will then need to be routed to the original destination.
- f. Redirect: Traffic designated by the Government to be blocked or otherwise undeliverable shall be routed to a device managed by HPCMP. This device will dead end the traffic and produce a meaningful response to the originator giving information that the traffic is blocked and additional information useful for getting an exception by the HPCMP.

In all cases the Contractor shall provide details and methods to accomplish the above capabilities designed to improve security.

12.10. Certification and Accreditation (C&A) support.

The Contractor shall support the C&A process as delineated in the approved DIACAP Package. 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 DoD Instruction 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP). 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 all problems resulting from the security certification and accreditation process including vulnerability assessments in accordance with the HPCMP comprehensive security assessment test plan. 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.

12.11. DIACAP package

The Contractor shall prepare and deliver a DIACAP package to the Government. The Contractor shall also maintain and continually update the DIACAP package throughout the life of the contract. The DIACAP package shall continually reflect the physical and logical configuration and security status of the DREN and its supporting components. The Contractor shall deliver all initial artifacts for the DIACAP package within 60 days after receipt of first delivery order. The DIACAP package shall consist of at least the following artifacts:

- a. DIACAP System Identification Profile (SIP) for all DREN WAN entities and all Contractor support locations that connect to DREN.
- b. DIACAP Scorecard for all DREN WAN entities and all Contractor support locations that connect to DREN.
- c. DIACAP Implementation Plan (DIP) for all DREN WAN entities and all Contractor support locations that connect to DREN.
- d. Physical Security Plan for all non-customer DREN hardware deployment, contract and support locations that connect to DREN.
- e. DREN System architecture and functionality description to include system capabilities and system criticality as well as unique / non-standard functionality descriptions as the DREN is modified throughout the life of the contract for each of the following:
 - DREN Service Delivery Points.
 - DREN WAN.
 - DREN Network Operations Center(s).

- DREN Test Center.
 - Commercial Transport Network.
- f. Documentation describing how required DoD Instruction 8500.2 IA Controls are met for all DREN WAN entities and all Contractor support locations that connect to DREN.
 - g. System Level IT Security POA&M for all DREN WAN entities and all Contractor support locations that connect to DREN.
 - h. Information System Security Requirements and Policy for all DREN WAN entities and all Contractor support locations that connect to DREN.
 - i. Security Concept of Operations for the following:
 - j. DREN SDP Components.
 - k. DREN WAN Components.
 - l. Network Operations Centers / Help Desk Centers.
 - m. Out-of-Band Network Management & Government Furnished Equipment (GFE).
 - n. Commercial Transmission Facilities.
 - o. Network Management.
 - p. Disaster Recovery.
 - q. DREN Hardware Management and Access Security Policy and Procedures.
 - r. Local and Wide Area Network Security Policy.
 - s. Security Requirements Traceability Requirements Matrix to include User IA training, SA training and Certification and IA personnel Training & Certification.
 - t. Baseline network device, access control lists, firewall and host configurations.
 - u. Configuration Management Plan for all DREN WAN entities and all Contractor support locations that connect to DREN.
 - v. Connection Approval Process for all Contractor support locations that connect to DREN.
 - w. Restricted area access lists for all Contractor support locations that connect to DREN.
 - x. Access lists for File systems.
 - y. Personnel Security Policy.
 - z. User Agreement Policy.
 - aa. Hardware and software lists for all DREN WAN entities and all Contractor support locations that connect to DREN.

- bb. Antivirus Policy for all Contractor support locations that connect to DREN.
- cc. Audit Procedures and Policy.
- dd. Identification & Authentication Policy and Procedures.
- ee. Intrusion Detection Policy.
- ff. Emergency Response and Incident Audit Reporting Plan and Procedures all DREN WAN entities and all Contractor support locations that connect to DREN.
- gg. Security Incident Reporting Procedures.
- hh. Configuration and Change Management Process Policy and Procedures.
- ii. Logical network diagrams that include all Contractor support locations that connect to DREN as well as the standard logical layout of all DREN WAN entities to include non-standard logical layout diagrams.
- jj. Policies and procedures for implementing Joint Task Force - Global Network Operations (JTF-GNO) Information Assurance Vulnerability Alerts (IAVA), applicable Communications Tasking Orders (CTOs) and applicable Operational Directive Messages.

12.12. Security Test and Evaluation Plan.

The Contractor shall develop 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 DIACAP Package. The test plan and procedures shall be provided to the Government for approval.

12.13. Security Operations.

12.13.1. Network Management Data.

The Contractor shall provide and ensure 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. 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 / sub-network 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.

12.13.2. 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.. 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. The Contractor shall define the process for providing access privileges to Government personnel on a need to know basis.

12.13.3. Service Protection.

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 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 an 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

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 number and location of sensors. Sensor placement will vary over time based on network architecture, Collectives and communities of interest, and other factors as described in the Attachment D, Separation and Protection, and Attachment E, Collectives

12.13.4. Security Incident Reporting.

The Contractor shall provide security incidence reporting in coordination 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. Coordinating with HPCMP Security and its components, such as the 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.

12.13.5. 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 and it's supporting facilities at no additional cost to the Government. In addition, specific extraordinary vulnerabilities may be negotiated at the Government's request or discretion.

12.13.6. 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 by 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.

12.13.7. Continuity of Operations.

The Contractor shall provide security management plans and functionality for the protection of the integrity of DREN and associated resources, including plans to prevent malicious Internet attacks from reaching DREN. The Contractor shall develop a Computer/System Emergency Response Plan detailing Contractor operating procedures, plans for operating during emergency situations, and plans for the restoration of transmission services in the event of a disaster.

12.13.8. 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.

Attachment A

ACRONYMS

ANSI	American National Standards Institute
ARC	Affiliated Resource Center
ASD (NII)	Assistant Secretary of Defense (Networks and Information Integration)
ASN	Autonomous System Number
ASON	Automatically Switched Optical Network
ASTN	Automatic Switched Transport Network
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
C&A	Certification and Accreditation
CCB	Configuration Control Board
CDRL	Contract Data Requirements List
CER	Cell Error Rate
CERT	Computer Emergency Response Team
CLIN	Contract Line Item Number
CNDSP	Computer Network Defense Service Provider
CO	Contracting Officer
COI	Communities of Interest
COMSEC	Communications Security
CONUS	Continental United States
COOP	Continuity of Operations
CPE	Customer Premise Equipment
DAMP	DREN Active Measurement Program
DDOE	Defense Information Systems Agency Direct Order Entry
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISN-LES	Defense Information Systems Network-Leading Edge Services
DNS	Domain Name System
DO	Delivery Order
DoD	Department of Defense
DRAGON	Dynamic Resource via GMPLS Optical Networks
DREN	Defense Research and Engineering Network
DS	Digital Service
DSRC	Department of Defense Supercomputing Resource Center
DT&E	Development Test and Evaluation

DWCF	Defense Working Capital Fund
ESnet	Energy Sciences Network
ET	Eastern Time
FAR	Federal Acquisition Regulation
FFP	Firm-Fixed-Price
FOIA	Freedom of Information Act
Gbps	Gigabits per second
GFP	Generic Framing Procedures
GIG	Global Information Grid
GMPLS	Generalized Multiple Protocol Label Switching
GSA	General Services Administration
GUI	Graphical User Interface
HPC	High Performance Computing
HPCMP	High Performance Computing Modernization Program
HPCMPO	High Performance Computing Modernization Program Office
HVAC	Heating, Ventilating, and Air-Conditioning
I-KPP	Interoperability Key Performance Parameter
I&A	Identification and Authentication
IA	Information Assurance
IAB	Internet Architecture Board
IAVA	Information Assurance Vulnerability Alert
ICMP	Internet Control and Management Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocols
IO	Information Operations
IP	Internet Protocol
IPC	Initial Performance Capability
IPSEC	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISOO	Information Security Oversight Office
ISP	Internet Service Provider
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
JFCOM	US Joint Forces Command
JITC	Joint Interoperability Test Command
JMETC	Joint Mission Environment Test Capability

JTF-GNO	Joint Task Force-Global Network Operations
LCC	Local Control Center
LEC	Local Exchange Carrier
M&S	Modeling and Simulation
MAN	Metropolitan Area Network
MDA	Missile Defense Agency
MLD	Multicast Listener Discovery
MRC	Monthly Recurring Charge
NAC	National Agency Check
NACI	National Agency Check plus written Inquiries
NAP	Network Access Point
NASA	National Aeronautics Space Administration
NIC	Network Information Center
NISPOM	National Industrial Security Program Operating Manual
NMS	Network Management Station
NOC	Network Operations Center
NRC	Non-Recurring Costs
NSA	National Security Agency
O&M	Operations and Maintenance
OAM	Operation, Administration, and Management
OCONUS	Outside Continental US
OSI	Open System Interconnection
OTU	Optical Transport Unit
OVS	Optical Wavelength Service
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POTS	Plain Old Telephone Service
QoS	Quality of Service
RDI	Remote Defect Indication
RDT&E	Research, Development, Test And Evaluation
RFI	Request for Information
RSVP	Resource ReSerVation Protocol
S&T	Science and Technology
SBIR	Small Business Innovation Research
SDP	Service Delivery Point

SDREN	Secret Defense Research and Engineering Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SOW	Statement of Work
SPI	Software Protection Initiative
SR	Service Request
SSAA	System Security Authorization Agreement
SSL	Secure Socket Layer
ST&E	Security Test and Evaluation
STRATCOM	US Strategic Command
T&E	Test and Evaluation
TAP	Technical Advisory Panel
TEMP	Test and Evaluation Master Plan
TI	Technical Insertion
TIP	Technology Insertion Proposal
TT	Trouble Ticket
USGS	US Geological Survey
vBNS	Internet, National Science Foundation Network
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
WAN	Wide Area Network or Wide Area Networking

Attachment B

CURRENT DREN SITES

Site_Name	IPC Category	Site_Class	NPA_NXX	DREN II Bandwidth
AK, Fairbanks (ARSC)	B	HPCMP-DSRC	907-474	OC-12
HI, Kihei (Maui) (MHPCC)	B	HPCMP-DSRC	808-874	OC-12
MD, Aberdeen Proving Ground (ARL-APG)	A	HPCMP-DSRC	410-278	OC-48
MS, Stennis Space Center (NAVO)	A	HPCMP-DSRC	228-688	OC-48
MS, Vicksburg (ERDC)	A	HPCMP-DSRC	601-634	OC-48
OH, Wright-Patterson AFB (AFRL)	A	HPCMP-DSRC	937-257	OC-48
AL, Redstone Arsenal (SMDC)	B	HPCMP-ARC	256-842	OC-12
CA, San Diego (SSC-SD)	A	HPCMP-ARC	619-553	OC-48
DC, Naval Research Lab (NRL)	A	HPCMP-ARC	202-767	OC-48
NY, Rome (AFRL/IF)	C	HPCMP-ARC	315-330	OC-3
AK, Fort Greely (CRTC)		RDT&E	907-873	DS-3
AK, South Anchorage (National Park Service)		RDT&E	907-644	
AL, Fort Rucker (USAAVNC)	C	HPCMP	334-255	DS-3
AL, Huntsville (MDA-TH-TC)		RDT&E	256-955	DS-3
AL, Huntsville (SMDC-ARC)	C	RDT&E	256-922	OC-3
AL, Maxwell AFB (ACSC)	C	HPCMP	334-953	DS-3
AL, Redstone Arsenal (MDA)		RDT&E	256-824	OC-12
AZ, Fort Huachuca (EPG)	C	HPCMP	520-533	OC-3

AZ, Goodyear (LMC)		RDT&E	623-925	DS-3
AZ, Mesa (AFRL-MRS)	C	HPCMP	480-988	DS-3
AZ, Scottsdale (GD C4 Systems)		RDT&E	480-441	DS-3
AZ, Tucson (Raytheon)	C	RDT&E	520-794	OC-3
AZ, Yuma Proving Ground (YPG)	C	HPCMP	928-328	OC-3
CA, Anaheim (Boeing MDA)		RDT&E	714-762	DS-3
CA, Camp Pendleton (MCCTSA)		RDT&E	760-725	DS-3
CA, China Lake (NAWC-WD)	B	HPCMP	760-939	OC-12
CA, Edwards AFB (AFRL-PR)	B	HPCMP	661-277	OC-12
CA, El Segundo (NG)		RDT&E	310-331	DS-3
CA, El Segundo (Raytheon)		RDT&E	310-334	OC-12
CA, Huntington Beach (Boeing FCS)		RDT&E	714-896	OC-3
CA, Los Angeles AFB (MDS-STSS)		RDT&E	310-653	OC-3
CA, Monterey (NPS)	C	HPCMP	831-656	OC-3
CA, Monterey (NRL-MRY)	B	HPCMP	831-656	OC-12
CA, Norco (NSWC Corona)		RDT&E	951-273	DS-3
CA, Palmdale		RDT&E	661-572	DS-3
CA, Point Mugu (NAWC-WD)	C	HPCMP	760-989	OC-3
CA, Port Hueneme (NFESC)	C	HPCMP	805-982	OC-3
CA, Redondo Beach (NG MDA)		RDT&E	310-812	DS-3

CA, San Diego (NG)		RDT&E	858-592	DS-3
CA, Sunnyvale (LMC MDA)		RDT&E	408-742	DS-3
CA, Vandenberg (MDA-GMI)		RDT&E	805-606	OC-3
CA, Woodland Hills (ATK)		RDT&E	818-887	DS-3
CO, Colorado Springs (SMDC-CS)		RDT&E	719-554	DS-3
CO, Denver (LMC)		RDT&E	303-430	OC-3
CO, Littleton (LMC)		RDT&E	303-705	DS-3
CO, Schriever AFB (MDIOC)	B	HPCMP	719-567	OC-12
CO, US Air Force Academy (USAFA)	B	HPCMP	719-333	OC-12
DC, Navy Yard (SPAWAR)		RDT&E	202-685	DS-3
DC, Pentagon (DOT&E)	C	HPCMP	703-692	DS-3
DC, Vermont Ave (DHS)		RDT&E	202-254	OC-3
FL, Eglin AFB (96th CG)	C	HPCMP	850-882	OC-12
FL, MacDill AFB (SOCOM)		RDT&E	813-828	DS-3
FL, Melbourne (SSF)		RDT&E	321-951	DS-3

FL, Orlando (LMC MF&FC)		RDT&E	407-356	DS-3
FL, Orlando (NAWC-TSD)	C	RDT&E	407-380	DS-3
FL, Panama City (CSS)	C	HPCMP	850-235	DS-3
FL, Tyndall AFB (AFRL-MLQ)	C	HPCMP	850-283	DS-3
GA, Fort Benning (USAIC)	C	RDT&E	706-545	DS-3
GA, Fort Gordon (USASC)		RDT&E	706-791	OC-3
HI, Barking Sands (PMRF)	B	RDT&E	808-337	OC-12
HI, Manoa (Oahu)	B	RDT&E	808-653	OC-12
HI, Pearl City (Oahu)	B	RDT&E	808-455	OC-12
IL, Champaign (CERL)	C	HPCMP	217-373	DS-3
IL, Scott AFB (AFCA)		RDT&E	618-229	DS-3
IL, West Chicago (Morgan Franklin MDA)		RDT&E	630-562	DS-3
IN, Crane (NSWC Crane)		RDT&E	812-854	DS-3
IN, Fort Wayne (Raytheon)		RDT&E	260-429	DS-3
KS, Fort Leavenworth (USACAC)		RDT&E	913-684	OC-3
KY, Fort Knox (USAARMC)	C	RDT&E	502-942	OC-3

MA, Chelmsford (Goodrich)		RDT&E	978-967	DS-3
MA, Hanscom AFB (AFRL)	C	HPCMP	508-233	OC-3
MA, Natick (SSC)	C	HPCMP	508-233	DS-3
MA, Woburn (Raytheon MDA)		RDT&E	339-645	DS-3
MD, Aberdeen Proving Ground (RDECOM)		RDT&E	410-436	OC-3
MD, Adelphi (ARL-ALC)	B	HPCMP	301-394	OC-12
MD, Annapolis (USNA)	B	HPCMP	410-293	OC-12
MD, Bethesda (NSWC-CD)	C	HPCMP	301-227	OC-3
MD, Fort Detrick (USAMRIID)	C	HPCMP	301-619	DS-3
MD, Fort Meade (IORANGE)		RDT&E	443-477	DS-3
MD, Indian Head (NSWC)	C	HPCMP	301-743	OC-3
MD, Laurel (JHUAPL)		RDT&E	240-228	OC-3
MD, Linthicum (NG)		RDT&E	410-765	DS-3
MD, Patuxent River (NAWC-AD)	B	HPCMP	301-342	OC-12
MD, Silver Spring (WRAIR)	C	HPCMP	301-319	DS-3
MI, Warren (TACOM)	C	HPCMP	810-574	DS-3
MO, Berkley (Boeing FCS)		RDT&E	314-232	OC-3
MO, Fort Leonard Wood (USAMSC)		RDT&E	573-563	DS-3
MO, Hazlewood (Boeing)		RDT&E	314-895	OC-12
MO, Kansas City (MCEITS)		RDT&E	816-361	DS-3

MO, Whiteman AFB		RDT&E	660-687	DS-3
NC, Durham (RTP-ARO)	C	HPCMP	919-549	DS-3
NC, Fort Bragg (ARSOBL)		RDT&E	910-296	DS-3
NE, Offutt AFB (AFWA)	C	HPCMP	402-294	OC-3
NH, Hanover (CREEL)	C	HPCMP	603-646	DS-3
NJ, Fort Monmouth (CERDEC)	C	HPCMP	732-532	OC-3
NJ, Lakehurst (NAWC-AD)	C	RDT&E	732-323	OC-3
NJ, Morrestown (NSWC LCS MPDP)		RDT&E	856-772	DS-3
NJ, Picatinny Arsenal (ARDEC)	C	HPCMP	973-724	DS-3
NJ, Wayne (BAE Systems)		RDT&E	973-663	DS-3
NM, Albuquerque (Boeing MDA)		RDT&E	505-449	DS-3
NM, Holloman AFB (NAVAIR)		RDT&E	505-572	OC-3
NM, Kirtland AFB (AFRL)	C	HPCMP	505-846	OC-3
NM, Las Cruces (NASA White Sands)		RDT&E	575-527	OC-3
NM, Playas (Training & Research Ctr)		RDT&E	505-436	DS-3
NM, White Sands (WSMR)	B	HPCMP	505-678	OC-12
NV, Nellis AFB (28th TS)		RDT&E	702-652	OC-12

NY, Bethpage (NG)		RDT&E	516-575	DS-3
NY, Watervliet Arsenal (Benet Lab)	C	HPCMP	518-266	DS-3
NY, West Point (USMA)	B	HPCMP	845-938	OC-12
OH, Beavercreek (AT-SPI)		RDT&E	937-320	DS-3
OH, Beavercreek (SAIC)		RDT&E	937-431	DS-3
OK, Fort Sill (USAFAC)		RDT&E	580-442	DS-3
OK, Tinker AFB (AWACS PTF)		RDT&E	405-734	DS-3
PA, New Cumberland (USALTA)		RDT&E	717-770	DS-3
PA, Philadelphia (NSWC-CD)		RDT&E	215-897	DS-3
PA, Philadelphia (SPAWAR PAC)		RDT&E	215-214	DS-3
RI, Newport (NUWC)	C	HPCMP	401-841	OC-3
SC, Charleston (SPAWAR)	C	HPCMP	843-974	OC-12
SC, North Charleston (WCI)	C	HPCMP	843-529	DS-3
TN, Arnold AFB (AEDC)	C	HPCMP	931-454	DS-3
TX, Arlington (Bell Helicopter NAVAIR)		RDT&E	817-280	DS-3
TX, Brooks AFB (AFRL-HE)	C	HPCMP	210-536	DS-3

VA, Arlington (AFOSR)	C	HPCMP	703-676	DS-3
VA, Arlington (LMC)		RDT&E	703-413	OC-3
VA, Arlington (NELO)		RDT&E	703-602	DS-3
VA, Dahlgren (NSWC)	C	HPCMP	540-653	OC-3
VA, Dulles (Raytheon)		RDT&E	571-226	DS-3
VA, Fort Belvoir (CIO-MDW)	B	HPCMP	703-704	OC-12
VA, Fort Lee (USACASC)		RDT&E	804-765	DS-3
VA, Fort Monroe (TRADOC)		RDT&E	757-788	DS-3
VA, Langley AFB		RDT&E	757-322	DS-3
VA, Lorton (HPCMPO)	C	HPCMP	703-493	OC-3
VA, Newport News (JTCOIC)		RDT&E	757-322	DS-3
VA, Norfolk (COMOPTEVFOR)		RDT&E	757-282	DS-3
VA, Norfolk (SPAWAR)		RDT&E	757-443	OC-3
VA, Portsmouth (SPAWAR)		RDT&E	757-558	DS-3
VA, Quantico (MCNOSC)		RDT&E	703-784	DS-3
VA, Radford (ALTESS)		RDT&E	540-731	DS-3
VA, Stafford (ITSFAC)		RDT&E	703-221	DS-3
VA, Suffolk (JNTC)		RDT&E	757-203	OC-3
VA, Vienna (HPCMPO)	C	HPCMP	703-749	DS-3

VA, Virginia Beach (NSWC Damneck)		RDT&E	757-492	OC-3
VA, Wallops Island (SCSC)		RDT&E	757-854	OC-3
WA, Fort Lewis (ATEC)		RDT&E	253-967	DS-3
WA, Keyport (NUWDC)		RDT&E	360-396	DS-3
WA, Tukwila (Boeing MDA)		RDT&E	206-655	OC-3
CA, Los Angeles (Equinix)		NAP	312-727	
CA, Moffett Field (NASA Ames - MAE West)		NAP	650-604	OC-3
IL, Chicago (StarLight, Optical Star)		NAP	312-727	OC-12
MD, College Park (NGIX-East)		NAP	301-405	OC-12
VA, Ashburn (Equinix)		NAP	650-604	
WA, Seattle (PNWGP)		NAP	206-443	OC-12
AK, Fort Richardson		Future	907-428	
AL, Mobile (UROC)		Future	251-690	
Australia, Bungendore		Future		
Australia, Canberra		Future		
CA, Fort Irwin		Future	760-380	
CA, Newport Beach (Universal Space Network)		Future	949-476	
CA, Rancho Bernado (NG)		Future	858-618	

NM, Albuquerque (Honeywell FCS)		Future	505-828	
CA, San Diego (Raytheon)		Future	858-571	
CO, Colorado Springs (Intelligent Software Solutions)		Future	719-457	
CO, Peterson AFB		Future	719-556	
CT, Norwalk		Future	516-346	
DC, Washington (NDU)		Future	202-685	
DC, Washington (USNO)		Future	202-762	
DE, New Castle		Future	302-323	
FL, Hurlburt Field		Future	850-844	
GA, Fort Stewart		Future	912-435	
GA, Warner Robins AFB		Future	478-222	
Germany, Ramstein Air Base		Future		
Germany, Stuttgart (Mantech Patch Barracks)		Future		
ID, Idaho Falls (Idaho National Lab)		Future	208-526	
IL, Urbana (Petascale Computing Facility)		Future	217-244	
IN, Butlerville, (Muscatatuck UTC)		Future	317-247	
KS, McConnell AFB		Future	316-759	
KY, Lexington (L-3 Communications)		Future	859-293	
KY, Louisville (NSWC)		Future	502-364	
LA, New Orleans (SPAWAR)		Future	504-218	
MA, Bedford (MITRE)		Future	781-271	
MA, Lexington (Atmospheric & Environmental Research)		Future	781-761	

MD, College Park (NARA)		Future	301-837	
MD, Fort Washington		Future	301-203	
MD, Linthicum (DCGS-A2)		Future	301-483	
NC, Camp Lejeune (MCIEAST)		Future	910-451	
NH, Nashua (BAE)		Future	603-885	
NJ, Atlantic City (FAA TC)		Future	609-485	
NM, Albuquerque (NAWCWD)		Future	505-883	
NY, Fort Drum (BCTC)		Future	315-772	
PA, McKees Rocks		Future	412-777	
Spain, Moron Air Base		Future		
TN, Millington (Naval Spt Activity)		Future	901-874	
TN, Pulaski		Future	931-363	
TX, Castle Hills (CME)		Future	210-492	
TX, Fort Sam Houston		Future	210-221	
TX, Houston (Boeing/FCS)		Future	281-244	
TX, Randolph AFB		Future	210-652	
VA, Alexandria (ERDC TEC)		Future	703-428	
VA, Arlington (JPO)		Future	703-602	
VA, Arlington (JSF Program Office)		Future	703-602	
VA, Arlington (OSD CAPE SAC)		Future	703-699	
VA, Chantilly (DCGS-IC)		Future	703-961	
VA, Ft Eustis		Future	757-878	
VA, Kingtown (SAIC)		Future	703-971	

VA, McLean (MITRE)		Future	703-983	
VA, Norfolk (NDU)		Future	757-443	
WV, Allegany Rocket Center (Ballistics Laboratory NARA)		Future	304-726	
FL, NAP of the Americas		NAP	206-443	
NY, NAP		NAP	718-355	
VA, McLean (L3 NAP)		NAP	703-762	
AL, Huntsville (MIT)		Future	256-721	
AL, Montgomery (Gunter Annex)		Future	334-416	
AZ, Mesa (FCS)		Future	480-891	
CA, Fallbrook		Future	760-731	
CA, Lemoore (NAS)		Future	559-998	
CA, Presidio of Monterey		Future	831-242	
CA, Santa Clara (FCS)		Future	408-289	
CT, Waterford (Sonalysts)		Future	860-442	
FL, Pensacola		Future	850-452	
GA, Atlanta (JMETC)		Future	404-407	
GA, Marietta (LMC)		Future	770-494	
HI, Honolulu (IO Range)		Future	808-838	
MA, Pittsfield (NSWC)		Future	413-494	

MD, Suitland		Future	301-669	
MI, Sterling Heights (FCS)		Future	586-825	
MN, Minneapolis (AHPARC)		Future	612-337	
MN, Minneapolis (FCS)		Future	763-572	
NV, Hawthorne		Future	775-945	
NY, Owego (LMC)		Future	607-751	
OH, Columbus		Future	614-692	
OK, Tinker AFB		Future	405-734	
PA, Carlisle (AWC)		Future	717-245	
PA, Philadelphia		Future	610-591	
PA, State College (Penn State)		Future	814-865	
RI, Quonset (IO Range)		Future	401-886	
TN, Memphis		Future	901-325	
TX, Richardson		Future	972-705	
UK, Portsdown		Future	607-751	
VA, Alexandria (IDA)		Future	703-845	
VA, Alexandria (WMEBL)		Future	703-924	
VA, Arlington (MDA-HQ)		Future	703-693	
VA, Newport News (NG)		Future	757-688	
VA, Reston (BAH)		Future	703-995	
VA, Reston (NGAPSL)		Future	703-262	
VA, Springfield		Future	703-440	
VA, Vienna (SAIC FCS)		Future	703-767	

VA, Virginia Beach (Sonalysts)		Future	757-490	
WA, Seattle (Boeing FCS)		Future	253-773	
WA, Silverdale		Future	360-396	
WV, Fairmont		Future	304-368	

Attachment C

CONCERNING PACKET LOSS REQUIREMENT

The DREN Performance Work Statement (PWS) gives the requirements for packet loss, stated as both not to exceed a value of 0.1% and also as a performance level necessary to sustain a high speed TCP/IP flow.

DREN is a high performance network and is required to deliver high data throughput between DREN sites. Bulk data flows almost always use the standard TCP/IP protocol. It is a requirement that data transfers are able to take full advantage of the DREN subscription rate (sustained and peak levels). In the case of a single TCP/IP flow (little or no other traffic) between two SDPs with the same access speed, that flow should operate at or above the “sustained” subscription rate. In the case of SDPs of unequal access speeds, the single TCP/IP flow should operate at the lesser of the two “sustained” subscription rates.

It is well known that TCP/IP performance is limited by such things as the link bandwidth and where the receive window is inadequate (less than the product of round trip time and bandwidth). More recent study of TCP performance by Mathis², Padhye³, and others has shown that TCP/IP performance is also bounded by a relationship between Max Transmission Unit (MTU), round trip time (RTT), and packet loss, as follows:

$$\text{bps} < (0.7 * \text{MTU} / (\text{RTT} * \text{sqrt}(\text{loss})))$$

While MTU is limited by the hardware technology (1500 bytes for Ethernet, or 9000 bytes for Gigabit Ethernet with jumbo frames), and the RTT has natural limits based on the speed of light in fiber, the only parameter left to “tune” to achieve high TCP/IP performance is the packet loss.

Based on the above models, very low packet loss is necessary in order for DREN to achieve acceptable TCP/IP performance. The desire is to specify a minimum packet loss requirement that would allow DREN to achieve high-sustained TCP/IP rates under almost all conditions. Unfortunately, it is difficult to directly

² M. Mathis, J. Semske, J. Mahdavi, and T. Ott. The macro-scopic behavior of the TCP congestion avoidance algorithm. Computer Communication Review, 27(3), July 1997.

http://www.psc.edu/networking/papers/model_ccr97.ps

³ J. Padhye, V. Firoiu, D. Towsley, J. Kurose (U.Mass) Modeling TCP Throughput: A Simple Model and its Empirical Validation

<http://www.acm.org/sigcomm/sigcomm98/tp/paper25.pdf>

measure loss in this range. However, the actual requirement is for DREN to provide a service that performs well enough to sustain TCP/IP flows at the “sustained” subscription rate or better.

So, instead of trying to deliver and measure a very low loss performance characteristic, the offeror must guarantee and demonstrate that the performance of the network will be such that a single TCP/IP flow will operate at or above the “sustained” subscription rate between computers connected at any two SDPs, given a well behaved and properly tuned standards compliant off-the shelf TCP/IP implementation in the computers at both ends.

The initial demonstration must include a wide area (preferably coast-to-coast) test between high bandwidth sites. The test must include a demonstration using appropriately-sized-Ethernet interfaces as separate tests. This test should be included as part of the Initial Performance Capability (IPC). Additional tests will be performed by the Government or at the request of the Government to verify continued delivery of this performance level between any two SDPs.

Attachment D

DISCUSSION OF SEPARATION AND PROTECTION

All information (data) being transported across DREN (data-in-transit) or stored on DREN (data-at-rest) must be protected to achieve an appropriate level of confidentiality, integrity, and availability. In a shared environment such as DREN, mechanisms must be in place to achieve the appropriate level of protection through separation of various portions of the network. DREN as a whole must be separated from any underlying commercial networks. Accredited enclaves must be separated from other enclaves at their accreditation boundary. DoD components must be separated from non-DoD components. Different levels or types of separation may be required for each situation.

In order to assure an appropriate level of confidentiality and integrity, various mechanisms can be employed, including encryption or various types of logical or physical separation. Some mechanisms are stronger than others. The stronger mechanisms are generally more costly or unwieldy than the weaker mechanisms, and may not be the best choice if a weaker mechanism is sufficient. Physical separation is generally stronger than logical separation. Encryption can be employed when sufficient separation is not possible.

The following types of “separation” are defined:

Physical separation	An isolation mechanism between segments of the network utilizing independent hardware or circuits that are not shared between the isolated segments. Examples include separate wires, lambdas, circuits, ports, switches, routers, and separate routing modules in a shared chassis.
Virtual separation	An isolation mechanism between segments of the network, where the hardware components of the network offer organic (internal) facilities to provide isolation between segments. Examples include VLANs, virtual circuits, virtual switches, and virtual routing and forwarding (VRF).
Layer 1 separation	Layer 1 refers to the physical layer of the OSI Seven Layer Model. This layer of separation is equivalent to “physical separation” as defined above.
Layer 2 separation	This refers to isolation at the data link layer, where independent data-link segments may share the same physical (layer 1) circuit, yet are isolated so that there is no crossover between them, nor is it possible to access one segment from another segment. Examples include VLANs, virtual circuits, layer-2 VPNs (l2vpn), pseudo-wires, virtual-cross-connect, MPLS LSPs, etc. This is generally weaker than Layer 1 separation.
Layer 3 separation	This refers to isolation at the network or “IP” layer, where independent IP networks may share the same data-link (layer 2) service or flow through the

same router, yet are isolated so that it is not possible to access one IP network from another. Examples include router ACLs or VRFs. This is generally weaker than Layer 2 separation.

Separation by encryption	This provides isolation between segments by encrypting entire network segments, using FIPS 140-2 validated AES (or better) technology. It can be used in conjunction with the other separation mechanisms described here, to add strength to some of the weaker mechanisms.
Strength of protection	For the purposes of this document only, the following strengths are defined:
Basic protection	This is the protection and separation necessary for proper operation of the network, and to comply with best current practices of the Internet such as BCP 84. This would apply to all IP components of DREN. Layer 3 separation is generally sufficient to meet this requirement.
Standard protection	This is the protection and separation that is sufficient to isolate segments or enclaves within the same collective and governance structure and classification level, but are under separate accreditation or require isolation for other reasons. For network segments that carry no sensitive or controlled information, this level is also sufficient for protection from those in other collectives or from the underlying commercial infrastructure. Layer 2 separation is generally sufficient to meet this requirement.
Strong protection	This is the protection and separation that is sufficient to isolate network segments carrying sensitive or controlled information from the public Internet or public access components of the network, or from each other, or from any underlying commercial network infrastructure. This is the mechanism required to isolate DoD accredited portions of the network from all other (non-DoD) portions. Either Layer 1 separation or encryption are currently sufficient to meet this requirement, although well managed and controlled Layer 2 separation may suffice in some cases.
Very strong protection	This is the protection and separation that is sufficient to isolate classified networks from networks of lower classification. This requires NSA Type 1 encryption, and is not a requirement of this contract. The Government will separately implement any such capabilities.

The above definitions provide a framework for the discussion of requirements within DREN, and do not supersede existing or emerging DoD or other policies. In particular, the emerging protection standards for Controlled Unclassified Information (CUI) will provide additional guidance for protecting such information, which dictates that CUI must remain in a controlled environment (i.e. closed or virtual private networks) or must be encrypted if it leaves a controlled environment. The intent of the “strong protection” is to provide a sufficiently controlled environment for CUI on DREN network segments.

Attachment E

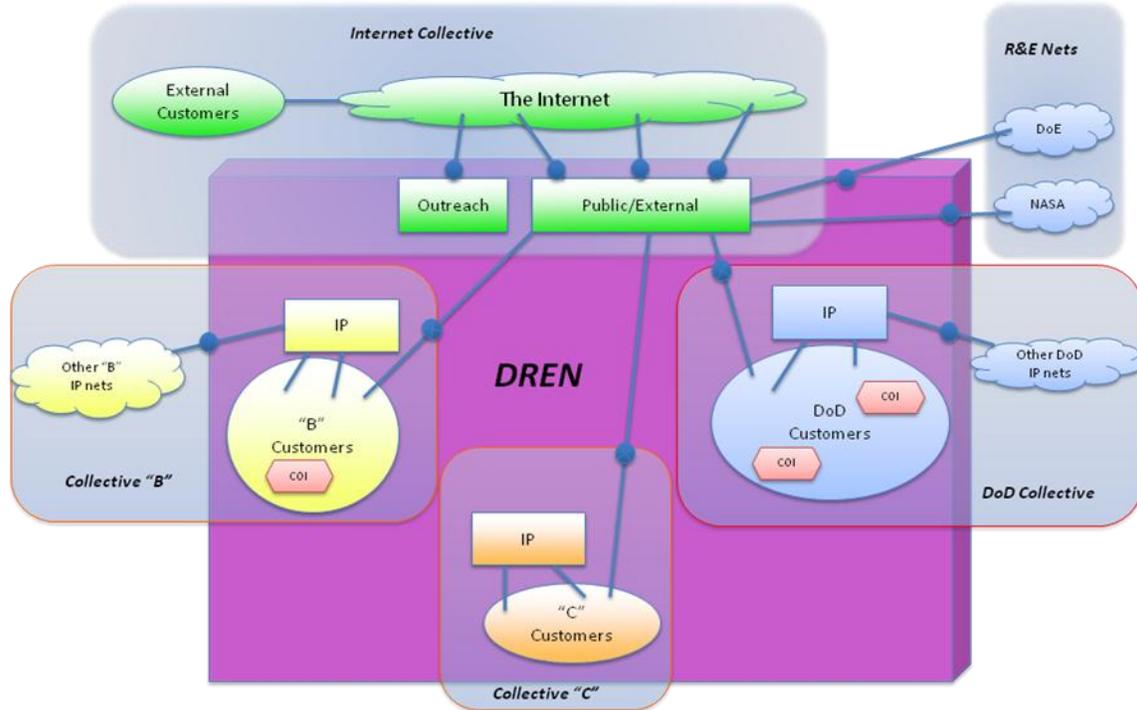
DISCUSSION OF COLLECTIVES

Each DREN customer is part of a larger grouping that has consistent over-arching governance (IA governance in particular) and other relationships, typically at the level of Federal Departments or Government Agencies. We refer to these as “collectives”. Each collective is generally independent of other collectives, and their governance may be very different from each other. The Department of Defense (DoD) is an example of a collective in this context. Each collective may include other approved wide area networks besides DREN, but all will be under the same IA governance regardless of where they obtain their network services. In the DoD collective, an example of an approved network external to DREN is NIPRNet.

DREN supports multiple collectives. Each collective typically requires the same types of services and architecture as every other collective, and requires direct connectivity between customers in the same collective (intra-collective) within strict SLAs (high performance, low latency, etc.). Within a collective, customers may be grouped into communities of interest (COI) that have even closer associations in support of organizational or mission requirements, and may require additional logical connectivity to support COI-unique functions. Traffic between collectives is also required, but with relaxed SLAs, and may just follow normal internet routing paths through various gateways. In some cases, private peering will be required to improve inter-collective traffic, or to keep it from transiting the public network.

The following figure (Figure Attachment E) provides a notional view of these concepts and how they relate to each other.

Figure Attachment E: Examples of Collectives



This figure shows that each collective includes customers on the DREN backbone, their own IP network interconnecting the customers in their collective, connections to other off-DREN networks that are in their collective, as well as some form of connectivity to the Internet to allow access from external customers and to allow DREN customers to access Internet content. Observe that collectives generally don't directly interconnect with each other, but can transit through the Public / External IP network on DREN, via gateways that provide IP routing and screening functions. Note that private peering is sometimes required to access other Research and Education networks, such as DoE and NASA.

Because of the non-equal IA governance of the collectives, they must be treated independently from each other (from a security perspective), and must be provided some level of isolation from each other even though they are operating across a shared network infrastructure, DREN, and any underlying commercial infrastructure supporting that. The required level of isolation between collectives must be in accordance with Table Attachment E.

Table Attachment E: Collective Governance and Protection Requirements

Collective	Governance	Protection between	Protection within
Internet	BCP84, consensus	Basic	Basic
DoD	DoD 8500.1	Strong	Standard
Collective “B”	Other	Standard	Standard
Collective “C”	Other	Standard	Standard
(etc.)			

The definitions of the various protection strengths can be found in Attachment D Separation and Protection. “Protection between” refers to the level of protection each collective must be provided, to protect it from other collectives and the underlying commercial infrastructure on which it is implemented. “Protection within” refers to the level of protection that must be provided between the instances of each DREN service (intra-collective IP service, Ethernet VLANs, etc.) that exists within a given collective.

For example, the IP service for the DoD collective only needs standard protection to separate it from one of the Ethernet service VLANs in the same collective, but must have strong protection from services in other collectives or from any commercial infrastructure over which this is implemented.

The existence of collectives may impact DREN performance metrics, such as latency. DREN’s SLA stipulates the minimum acceptable latency between any two DREN SDPs. However, if those two SDPs are in different collectives, then the IP traffic between them may need to exit via one gateway and re-enter elsewhere via another gateway. In such situations, the latency SLAs apply only to intra-collective traffic, and do not apply to inter-collective traffic. However, it is highly desirable to have inter-collective and other peering gateways located in multiple geographic regions to minimize the added latency from these interconnects, especially to the Internet collective from the others.

Attachment F

STANDARDS

Required Standards

Department of Defense Information Technology Standards Registry Baseline Release 09-2.0, July 30, 2009;

OMB Memorandum M10-15 FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management;

NIST publication SP-800-53 Revision 3 August 2009 and any subsequent publications that supersede it;

DoD Directive 4630.5, Interoperability and Supportability of Information Technology; (IT) and National Security Systems (NSS), May 5, 2004;

DoD IPv6 Standard Profiles for IPv6 Capable Products Version 4.0, July 30, 2009;

Telcordia GR 253 Synchronous Optical network (SONET) Transport Systems: Common Generic Criteria (10/09);

ITU-T Standards G.692 and G.694 Defining Optical Interfaces and Physical Layer Parameters for WDM Systems.

ITU-T H.323 Multimedia Over Packet;

ANSI T1.105, Telecommunications - Synchronous Optical Network (SONET) Basic Description Including Multiplex Structure, Rates and Formats

ATIS 0600107.2002 Digital Hierarchy - Formats Specifications, (Formerly ANSI T1.107

IEEE 802.3, 2008

IETF RFC-1191, Path MTU Discovery (11/1990);

IETF RFC-1305, Network Time Protocol (Version 3) Specification, Implementation, and Analysis (03/1992);

IETF RFC-1542, Clarifications and Extensions for the Bootstrap Protocol (10/1993);

IETF RFC-1738, Uniform Resource Locators (URL) (12/1994);

IETF Informational RFC 1770, IPv4 Option for Sender Directed Multi-Destination Delivery, (03/1995);

IETF RFC-1771, A Border Gateway Protocol 4 (BGP-4) (03/1995);

IETF RFC-1772, Application of the Border Gateway Protocol in the Internet (03/1995);

IETF RFC-1808, Relative Uniform Resource Locators (06/1995);

IETF RFC-1850, OSPF, Version 2, Management Information Base (11/1995);

IETF RFC-1918/BCP-5 Address Allocation for Private Internets, (02/1996);

IETF RFC-2131, Dynamic Host Configuration Protocol (03/1997);

IETF RFC-2236 Internet Group Management Protocol Version 2, (1997);

IETF RFC-2365/BCP-23 Administratively Scoped IP Multicast, (07/1998);

IETF RFC-2385 Protection of BGP Sessions via the TCP MD5 Signature Option, (08/1998);

IETF RFC 2401 Security Architecture for the Internet Protocol (11/1998);

IETF RFC 2411 Internet Protocol Security (IPSec) Document Roadmap (11/1998);

IETF RFC 2460 Internet Protocol Version 6 (IPv6) Specification (12/1998);

IETF RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, (12/1998);

IETF RFC-2475, An Architecture for Differentiated Services RFC 2597 Assured Forwarding PHB Group, (12/1998);

IETF RFC 2574, (SNMPv3) "The User-Based Security Model for Version 3 of the Simple Network Management Protocol (SNMP)", May 1999;

IETF RFC 2576, Coexistence between SNMP versions, (SNMPv1, SNMPv2, SNMPv3) March 2000;

IETF RFC 2575, "View-based Access Control Model for the Simple Network Management Protocol (SNMP)" (SNMPv3), May 1999;

IETF RFC-2616, Hypertext Transfer Protocol (HTTP)/1.1 (06/1999);

IETF RFC-2644, Requirements for IP Version 4 Routers (08/1999);

IETF RFC-2740, OSPF for IPv6, (12/1999);

IETF RFC-2790, Host Resources MIB (03/2000);

IETF RFC-2819, Remote Network Monitoring Management Information Base (05/2000);

IETF RFC-3140, Per Hop Behavior Identification Codes, (06/2001);

IETF RFC-3246 An Expedited Forwarding PHB, (03/2002);

IETF RFC-3260, New Terminology and Clarifications for Diffserv, (04/2002);

IETF RFC-3376, Internet Group Management Protocol, Version 3 (IGMPv3), (10/2002);

IETF RFC-3704/BCP-84, Ingress Filtering for Multihomed Networks, (03/2004);

IETF RFC-3871 Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure, (09/2004);

IETF RFC-3901/BCP-91 DNS IPv6 Transport Operational Guidelines, (09/2004);

IETF RFC-3945, Generalized Multi-Protocol Label Switching (GMPLS) Architecture, (10/2004);

IETF RFC-4033, DNS Security Introduction and Requirements (03/2005);

IETF RFC-4034, Resource Records for the DNS Security Extensions (03/2005);

IETF RFC-4035, Protocol Modifications for the DNS Security Extensions (03/2005);

IETF RFC-4594, Configuration Guidelines for DiffServ Service Classes, (08/2006);

IETF RFC-4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling, (01/2007);

IETF RFC-4762, Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling, (01/2007);

IETF RFC-4786/BCP-126 Operation of Anycast Services, (12/2006);

IETF RFC 5000 Internet Protocol Standard 1 Specification (05/2008);

IETF RFC-5681, TCP Congestion Control (09/2009);

IETF RFC-5635, Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF) (08/2009)

IETF Standard 13/RFC-1034/RFC-1035, Domain Name (11/1887);

IETF Standard 15/RFC-1157, Simple Network Management Protocol (SNMP) (05/1990)

IETF Standard 16/RFC-1155/RFC-1212, Structure and Identification of Management Information (05/90)/Concise MIB Definitions (03/1991)

IETF Standard 17/RFC-1213, Management Information Base for Network Management (03/1991);

IETF RFC-3700, Internet Official Protocol Standards (05/2008);

IETF Standard 37/RFC-0826, An Ethernet Address Resolution Protocol (11/1982);

IETF Standard 41/RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks (04/1984);

IETF Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112, Internet Protocol (09/1981);

IETF Standard 50/RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types (07/1994);

IETF Standard 54/RFC-2328, Open Shortest Path First Routing Version 2 (04/1998);

IETF Standard 6/RFC-768, User Datagram Protocol (UDP) (08/1980);

IETF Standard 7/RFC-793, Transmission Control Protocol (09/1981);

IETF Standard 8/RFC-854/RFC-855, TELNET Protocol (05/1983);

MIL-STD-2045-47001B, Connectionless Data Transfer Application Layer Standard, (01/98);

ITU-T G.709/Y.1331, Interfaces for the Optical Transport Network (03/2003);

ITU-T G.959.1, Optical Transport Network Physical Layer Interfaces (03/2006).

Optional Standards

ITU-T G.872, Architecture of Optical Transport Networks (2001);

ITU-T G.8080, Architecture for the Automatically Switched Optical Network (ASON);

ITU-T G.7712, Architecture and Specification of Data Communication Network, and Related ITU-T Recommendations G.7713X: Distributed Call and Connection Management; Distributed call and connection management based on PNNI; Distributed Call and Connection Management; Signaling mechanism using GMPLS RSVP-TE; Distributed Call and Connection Management; Signaling mechanism using GMPLS CR-LDP;

ITU-T Recommendation G.7714X: Generalized automatic discovery for transport entities; Protocol for automatic discovery in SDH and OTN networks;

ITU-T Recommendation G.7715X: Architecture and requirements for routing in the automatically switched optical networks; ASON routing architecture and requirements for link state protocols; ASON routing architecture and requirements for remote route query.

Sources of Standards

DoD Directive 5101.7, DoD Executive Agent for Information Technology Standards; DoDD 5101.7: "DoD Executive Agent for Information Technology Standards"

DoD Information Technology Standards Registry (DISR) is a repository of cited standards to be followed by DoD projects and deployments. This database can be accessed by authorized users via the web at <https://disronline.disa.mil/>

American National Standards Institute (ANSI): Order ANSI documents on-line at: <http://webstore.ansi.org>;

Internet Engineering Task Force (IETF): Order IETF documents on-line at: <http://tools.ietf.org/html>;

Institute of Electrical and Electronic Engineers (IEEE): Order IEEE documents on-line at: <http://standards.ieee.org>;

International Telecommunications Union (ITU): Order ITU documents on-line at: <http://www.itu.int/ITU-T/publications/recs.html>;

Telcordia: Order Telcordia documents on-line at: <http://telecom-info.telcordia.com/site-cgi/ido/index.html>;

Metropolitan Ethernet Forum: Order documents online at: <http://metroethernetforum.org>

Standards Provided as Reference

IETF RFC-2205, Resource ReSerVation Protocol (RSVP), (09/1997);

IETF RFC-2362. Protocol Independent Multicast – Sparse Mode (PIM-SM), (1998);

IETF RFC-2365. Administratively Scoped IP Multicast, (1998);

IETF RFC-1075. Distance Vector Multicast Routing Protocol, (1988);

IETF RFC-2715. Interoperability Rules for Multicast Routing Protocols, (1999);

RFCs pertaining to IPv6 (1886, 1891, 2080, 2373, 2374, 2428, 2460 - 2464, etc.)

RFCs pertaining to IP Flow Information Export (IPFIX) <http://www.ietf.org/dyn/wg/charter/ipfix-charter.html>

RFCs pertaining to IP Packet Sampling (PSAMP) <http://www.ietf.org/dyn/wg/charter/psamp-charter.html>

IETF-RFC-4111. Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)

Ethernet References:

802.1AE-2006 Media Access Control (MAC) Security, (08/2006);

802.1AX-2008 Link Aggregation, (11/2008);

802.1ad-2005 Virtual Bridged Local Area Networks Amendment 4: Provider Bridges, (05/2006);

802.1ag-2007 Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management, (12/2007);

802.1ah-2008 Virtual Bridged Local Area Networks Amendment 7: Provider Backbone Bridges, (08/2008);

802.1ah-2008 Virtual Bridged Local Area Networks, Link OAM, (08/2008);

802.1ap-2008 Virtual Bridged Local Area Networks Amendment 8: Management Information Base (MIB) Definitions for VLAN Bridges, (03/2009);

802.1D-2004 MAC Bridges, (06/2004);

802.1Q-2005 Virtual Bridged Local Area Networks, (05/2006);

802.1Qaw-2009 Virtual Bridged Local Area Networks Amendment 9: Management of Data Driven and Data Dependent Connectivity Faults, (07/2009);

802.1Qay-2009 Virtual Bridged Local Area Networks Amendment 10: Provider Backbone Bridge Traffic Engineering, (08/2009);

802.1X-2004 Port Based Network Access Control, (12/2004);

802.3-2008 Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Section One, (12/2008);

Technical Specification MEF 17 - Service OAM Requirements & Framework – Phase 1, April 2007

Technical Specification MEF 21 - Abstract Test Suite for UNI Type 2 Part 1: Link OAM, July 2008

Technical Specification MEF 6.1 - Ethernet Services Definitions - Phase 2, April 2008

Executive Documents

Presidential Memorandum, May 9, 2008, Designation and Sharing of Controlled Unclassified Information http://www.archives.gov/cui/documents/designation_cui.pdf

Presidential Memorandum, May 27, 2009, Classified Information and Controlled Unclassified Information <http://www.archives.gov/cui/documents/2009-presidential-memo.pdf>

Executive Order 12958, Classified National Security Information;

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

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

OMB Circular no. A-130, Management of Federal Information Resources.

Department of Defense Documents

DoD Directive 8500.1, Information Assurance (IA);

DoD Directive 8570 Information Assurance Training,

DoD Instruction 8500.2, Information Assurance (IA) Implementation;

DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP);
and

DoD Directive 8320.02, December 2, 2004, "Data Sharing in a Net-Centric Department of Defense".
<http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf>

DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM).

Computer Security Documents

Federal Information Processing Standards Publications (FIPS PUBS) Security Requirements for Cryptographic Modules (FIPS PUB 140-2).

Security Technical Implementation Guides

DISA Network Infrastructure Security Technical Implementation Guide (STIG)
<http://iase.disa.mil/stigs/index.html>

Operational Security Documents

Deputy Secretary of Defense Memorandum, DoD Information Assurance Vulnerability Alert (IAVA), 30 December 1999; and

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

Personnel Security Documents

DoD Regulation 5200.2-R, Personnel Security Program.

HPCMP References

DREN Service Agreement;

SDREN Connection Approval Process (CAP);

HPCMP Comprehensive Security Assessment Test Plan;

Attachment G

DATA DESCRIPTIONS

Title: Master Service Delivery Point (SDP) Plan / Individual SDP Report

The Master SDP Plan (6.2.2.8) and Individual SDP Reports (6.4.1) are used for planning, programming, and supporting DREN operations and maintenance, systems integration, and future engineering and installation efforts. These documents are also used in conjunction with facility records for other equipment commodities to ensure that complete records of DREN services on a base, station or facility are available.

The Master SDP Plan shall address at a minimum, the topics and reference the documents identified below. The Individual SDP Report shall be prepared in accordance with the Master SDP Plan and shall address site-specific details, including any variance from the standards documented in the Master SDP Plan.

1. Reference documents.
 - 1.1. Contract Performance Work Statement (PWS)
 - 1.2. Contractor's proposal incorporated as part of the contract upon award
 - 1.3. All applicable sections of local and state building codes
 - 1.4. Current versions of the following:
 - 1.4.1. National Electric Code
 - 1.4.2. American Institute of Steel Construction (AISC)
 - 1.4.3. American Welding Society (AWS).
 - 1.4.4. American Concrete Institute (ACI).
 - 1.4.5. Electronic Industries Association EIA Standard RS-232.
 - 1.4.6. American Society for Testing and Materials (ASTM).
 - 1.4.7. National Fire Protection Code (ANSI/NFPA-100).
 - 1.4.8. NFPA - National Electrical Code (ANSINEC-70).
 - 1.4.9. American Society of Heating, Refrigeration Air Conditioning Engineers' Code.
2. Format. The report shall be prepared in Contractor's format.

It shall be typewritten and is to be duplicated in non-fading ink.

- 2.1. The data indicated below shall be contained on the title page:
 - 2.1.1. Type of Report, Draft or Final
 - 2.1.2. Delivery Order Title and Number
 - 2.1.3. Date of the SDP Plan
 - 2.1.4. Version Number of the SDP Plan
 - 2.1.5. Security classification and distribution limitation markings shall be included on all pages.
3. Content.

- 3.1. Preliminary Information
 - 3.2. Revision History
 - 3.3. Table of Contents
 - 3.4. List of Figures
 - 3.5. List of Tables
 - 4. Detailed Information
 - 4.1. General Site Data
 - 4.1.1. Site Identification. This section should identify the following information regarding the site:
 - 4.1.2. DREN Contract Number
 - 4.1.3. Drop Shipping Address for the site, to include:
 - 4.1.3.1. Street Address
 - 4.1.3.2. City
 - 4.1.3.3. State
 - 4.1.3.4. Zip Code
 - 4.2. Primary Customer Representative (POC), to include:
 - 4.2.1. Name
 - 4.2.2. Commercial Telephone Number
 - 4.2.3. Fax Telephone Number
 - 4.2.4. Cell Telephone Number
 - 4.2.5. E-mail address
 - 4.3. Secondary Customer Representative (POC), to include:
 - 4.3.1. Name
 - 4.3.2. Commercial Telephone Number
 - 4.3.3. Fax Telephone Number
 - 4.3.4. Cell Telephone Number
 - 4.3.5. E-mail address

This section should justify any discrepancies between the Site Identification information provided and the corresponding information provided on the Request for Service (RFS) or Delivery Order (DO).

 - 4.4. Office Identification. This section should provide information for the Contractor Points of Contact responsible for the SDP and SDP Plan.
5. Applicable Documents
6. Power
 - 6.1. AC Power
7. Heating, Ventilating, And Air Conditioning (HVAC) Requirements
8. Plumbing Requirements
9. General
 - 9.1. Open Items

10. Site Alteration Sub-Plan (If Applicable)

- 10.1. Future SDP Upgrades
- 10.2. WAN Access Circuit
- 10.3. Additional Services

11. Installation / Modification Sub-Plan

- 11.1. Summary
- 11.2. SDP Equipment Description. This section includes:

11.2.1. Tables to include, but not necessarily limited to:

- 11.2.1.1. Original Equipment List;
- 11.2.1.2. Original Cable List;
- 11.2.1.3. Upgraded Equipment List;
- 11.2.1.4. Hardware Inventory, i.e., a “show chassis” report from the SDP equipment

11.2.2. Elevation view drawing of the equipment racks or cabinet identified on the floor plan drawing of the Site Survey. The drawing shall include arrangement of components, showing controls and indicators, layout of circuit cards, racks within the equipment, identification of card slots and cards, power distribution panels and other similar information necessary to characterize that equipment cabinet or rack.

11.2.3. Cross-connect drawing depicting wiring cross-connections between SDP equipment and components, i.e. customer premise or end user equipment.

- 11.3. Revised SDP Equipment Ordered
- 11.4. Cable Routing
- 11.5. Cable Management. This section includes cross-connect drawings depicting wiring cross-connections between SDP equipment and other components, i.e., jumpers on a distribution frame, building entrance terminals, to the commercial demarcation point. One drawing should depict the WAN circuit. One drawing should depict the POTS line circuit for Out-of-Band Management.

- 11.6. Installation Services
- 11.7. Space
- 11.8. Power
- 11.9. HVAC
- 11.10. Plumbing
- 11.11. Floor Loading
 - 11.11.1. Storage Space Requirements
 - 11.11.2. Impact Analysis

12. Acceptance Test Sub-Plan

- 12.1. Introduction
- 12.2. Testing Methodology
- 12.3. Reference SDP (SDP0)
- 12.4. Test Locations & Personnel

- 12.5. Initial Test And Acceptance
- 12.6. Site Activation & Individual Verification Testing For Initial Acceptance
- 12.7. DREN SDP Testing Matrix
- 12.8. Active Interfaces
- 12.9. Problem Identification And Resolution
- 12.10. Pass / Fail Criteria And Follow-Up Actions
- 12.11. DREN Test Problem Escalation
- 12.12. Problem Resolution
- 13. Termination / Restoration Sub-Plan
 - 13.1. General
 - 13.2. Purpose
 - 13.3. Equipment To Be Removed Upon Termination
 - 13.4. SDP Termination Impact Analysis
 - 13.5. Recommended SDP Site Termination Schedule
- 14. Instruction Sub-Plan
 - 14.1. General
 - 14.2. Purpose
 - 14.3. Procedure
 - 14.4. Instructional Services
 - 14.5. Recommended Type Of Training
 - 14.6. Training Computer Configuration Requirements
 - 14.7. Schedule
- 15. Site Survey
- 16. Process