Section C

PERFORMANCE WORK STATEMENT (PWS)

As of 19 Aug 2019

Contract Number	*(completed by the KO at time of contract or TO award)*
Task Order Number	Not Applicable
Contractor Name	*(completed by the KO at time of contract or TO award)*
Tracking Number	*(completed by the KO when complete package is received)*
Follow-on to Previous Contract and Task Order Number	Not Applicable

Table of Contents

1. Contracting Officer representative (COR) 8
2. Contract Title 8
3. Background 8
3.1. DREN Evolution 9
3.2. DREN Technical Leadership 10
4. Objectives 10
5. Scope 10
5.1. DREN4 Program Objectives 10
5.2. Continuation of DREN Services 11
5.3. Service Locations and Duty Hours 11
5.4. Synopsis of Future Network 11
6. Performance Requirements 12
6.0. Base Requirements for All Tasks 15
6.0.1. Hardware and Software 15
6.0.2. General Guidance 15
6.1. DREN Transport 15
6.1.0. Elements of Base Task 16
6.1.0.1. Collectives 16
6.1.0.2. Performance 17
6.1.0.3. Buffering 18
6.1.1. Ethernet 18
6.1.1.1. Switching 18
6.1.1.2. Multicast 18
6.1.1.3. Ethernet Quality of Service (QOS) 19
6.1.1.4. VLAN 19
6.1.1.5. Encryption 19
6.1.1.6. Frame Size 19
6.1.1.7. Ethernet Resiliency 20
6.1.2. Internet Protocol (IP) Transport 20
6.1.2.1. IPv6 20
6.1.2.2. IPv4 20
6.1.2.3. IP Maximum Transmission Unit (MTU) 21
6.1.2.4. Unicast 21
6.1.2.5. Multicast 21
6.1.2.6. Anycast 21
6.1.2.7. IP Quality of Service (QoS) 22
6.1.2.8. Multiple IP networks 22
6.1.2.8.1. Public External (PX) IP Network 22
6.1.2.8.2. DoD Only (DO) IP Network 22

6.1.2.8.3. Non-DoD Access (ND) Network 22
6.1.2.8.4. Extended DMZ (ED) Network 23
6.1.2.8.5. Management Networks 23
6.1.2.9. IP Routing 23
6.1.2.9.1. Best Current Practices 23
6.1.2.9.2. Routing Protocols 23
6.1.2.9.3. Peering 23
6.1.2.9.4. Architecture 24
6.1.2.9.5. Security Gateways (SGs) 25
6.1.2.9.6. Route Filtering 25
6.1.2.10. Controls, Policies, and Filtering 26
6.1.2.11. Internet Transit Service (ITS) (Separately Orderable) 27
6.1.2.11.1. Full Internet Transit 27
6.1.2.11.2. Outreach 27
6.1.2.11.2.1. Outreach Peering and Routing 27
6.1.2.11.2.2. Outreach Transport 28
6.1.3. Transport Performance 28
6.1.3.1. Latency 28
6.1.3.2. Jitter 29
6.1.3.3. Loss 29
6.1.3.4. Throughput 30
6.1.3.5. DCN Placement 30
6.1.3.6. Measurement and Testing 32
6.1.3.6.1. Latency Test 33
6.1.3.6.2. Pairwise TCP Test 33
6.1.3.6.3. Aggregate TCP Test 34
6.1.3.6.4. Pairwise Throughput Test 34
6.1.3.6.5. Aggregate Throughput Test 35
6.1.3.7. Degradation/Outage 35
6.2. DREN Node 35
6.2.0. Elements of Base Task 36
6.2.0.1. Government Data and Access Requirements 36
6.2.0.1.1. Flow 36
6.2.0.1.2. Log 36
6.2.0.1.3. Simple Network Management Protocol (SNMP) 36
6.2.0.1.4. BGP 37
6.2.0.1.5. Government Access to Network Components 37
6.2.0.2. DREN Node Types 37
6.2.0.2.1. Service Delivery Point (SDP) 37
6.2.0.2.2. DREN Core Node (DCN) 38
6.2.0.2.3. DREN eXchange Point (DXP) 38
6.2.0.3. DREN Node Line Rate 38

6.2.0.4. Physical Security at DCN and DXP Locations 39
6.2.1. Switch Function (One included) 39
6.2.1.1. Ports (Separately Orderable) 40
6.2.1.2. Modules (Separately Orderable) 40
6.2.1.3. Interconnections 41
6.2.1.4. Additional Switch Functions (Separately Orderable) 41
6.2.2. Router Function (Separately Orderable) 41
6.2.3. Firewall Function (Separately Orderable) 42
6.2.4. Compute Function (Separately Orderable) 43
6.2.4.1. Generic Compute Function 43
6.2.4.2. DAMP Compute Function 44
6.2.4.3. DJS Compute Function 45
6.2.5. Orchestration 45
6.2.5.1. Orchestrator 46
6.2.6. Internet Peering and Transit 46
6.2.6.1. Private Peering 46
6.2.6.1.1. Colocation and Cross connects at DXP locations 47
6.2.6.1.1.1. Colocation 47
6.2.6.1.2. Cross-Connects 47
6.2.7. Rack Space (separately orderable) 47
6.2.8. Passive Tap (separately orderable) 48
6.2.9. SDP Lite (SDP-L) 48
6.2.10. Tunnel Termination Point (TTP) (Separately Orderable) 50
6.3. Security 51
6.3.1. RMF Support 53
6.3.1.1. RMF IATT Package 56
6.3.1.2. RMF ATO Package 57
6.3.1.2.1. Systems Security Plan 58
6.3.1.3. Continuous Monitoring 59
6.3.2. Configuration Control Board Change Requests 61
6.3.3. Network Protections 62
6.3.4. Initial Boundary Protection Deployment 62
6.3.5. INFOCON/CPCON Changes 62
6.3.6. Intrusion Detection Systems (IDSs) 62
6.3.7. Network Management 62
6.3.8. SDREN 63
6.4. Management 65
6.4.1. Management Oversight 65
6.4.1.1. Program Management 65
6.4.1.2. Program Management Office 65
6.4.1.3. Project Management Planning and Control 66
6.4.1.4. Other Direct Cost (ODC) Management 66

6.4.1.5. Progress Reporting 66
6.4.1.6. DREN Meetings 67
6.4.1.6.1. Technical Interchange Meeting (TIM) 67
6.4.1.6.2. Contract Status Meetings 67
6.4.1.6.3. Technical Advisory Panel (TAP) 67
6.4.1.7. Asset and Configuration Management 68
6.4.1.8. Program Management Review (PMR) 68
6.4.1.9. Annual Planning and Design Review 69
6.4.2. Network Status Reporting 70
6.4.3. Evolution of Services 71
6.4.3.1. Technology Insertion Proposal (TIP) 71
6.4.3.1.1. Commercial Solutions for Classified (CSfC) 72
6.4.3.1.2. Enhanced Cybersecurity Service (ECS) 72
6.4.3.1.3. Boundary Cloud Access Point(s) 72
6.4.3.1.4. Time Reference Service 72
6.4.3.1.5. Contractor provided localized commodity Internet service 73
6.4.3.1.6. Hybrid SDP 73
6.4.3.2. Upgrades 73
6.4.3.3. Technical Refresh and Life Cycle Engineering Support 73
6.4.4. Simulation and Test Labs (Requirements and Status) 73
6.4.5. Accounting Management 74
6.5. Support 74
6.5.1. Service Provisioning 74
6.5.2. Change Request Provisioning 76
6.5.3. Service Management System (SMS) 78
6.5.3.1. Tickets (other than "Service" type) 79
6.5.3.2. Tickets (Service) 80
6.5.4. Contractor Managed Network Database 81
6.5.5. Network Operations Center (NOC) 82
6.5.5.1. Notifications 84
6.5.5.1.1. Outage Notification Methods, Levels, and Intervals 84
6.5.5.1.2. Security Incident Notifications 86
6.5.5.1.3. Contractor-Initiated Maintenance Notifications 86
6.5.5.1.4. Subscriber-Initiated Maintenance Notifications 87
6.5.6. Problem Management 88
6.5.7. DREN Node Availability Requirement 90
6.5.7.1. DREN Node Outage State Determination 90
6.5.7.2. Individual DREN Node MRC Billing Credits 90
6.5.8. Network Availability 90
6.5.8.1. Adjusted Network Availability (ANA) Determination 91
6.5.8.2. ANA Total MRC Billing Credits 92
6.5.8.3. Network Availability Report 92

6.5.9. Problem Escalation 93
6.5.10. Data Access and Storage Requirements 94
6.5.10.1. DREN Network Dynamic Data 94
6.5.10.1.1. API 94
6.5.10.1.2. Looking Glass 95
6.5.10.1.3. Data Dashboard 96
6.5.10.1.4. Flow Tool 97
6.5.10.2. Government Documentation Repository 97
6.5.11. OOB Access 97
6.5.12. Regression Testing 98
6.5.13. DREN Node Documentation 100
6.5.13.1. DREN Node Master Plan 100
6.5.13.2. Individual DREN Node As-Built Reports 101
6.5.13.3. DREN Node Site Survey Template 102
6.5.13.4. DREN Node Site Surveys 103
6.5.13.5. DREN Node Location Modification Plan 104
6.5.14. Acceptance Testing 104
6.5.14.1. Acceptance Test Plan 104
6.5.14.2. Acceptance Test Report 105
6.5.14.3. Acceptance Procedures 106
6.5.14.4. Tools and Test, Measurement, and Diagnostics Equipment (TMDE) 106
6.5.15. DNS Service 106
6.5.16. Touch Labor 107
6.6. Implementation and Transition 107
6.6.1. Phase I 109
6.6.1.1. Initial Performance Capability (IPC) 110
6.6.1.1.1. IPC Plan 111
6.6.1.1.2. Requirements Traceability Matrix (RTM) 112
6.6.1.1.3. IPC Implementation 113
6.6.1.1.4. IPC Demonstration Plan (IPCDP) 113
6.6.1.1.5. IPC Test and Demonstration 114
6.6.1.1.6. IPC Demonstration Report (IPCDR) 114
6.6.1.2. Assess and Authorization Process 115
6.6.1.3. Comprehensive Implementation and Test Plan (CITP) Development 115
6.6.2. Phase II 116
6.6.2.1. CITP Execution 117
6.6.2.2. Subscriber Cutover 117
6.6.3. Contract Phase Out 117
6.6.3.1. Planning and Engineering Support 117
6.6.3.1.1. Development of Contract Phase-out Transition Plan 118
6.6.3.1.2. Updating, Validating, and Transferring of Support Documentation 118
6.6.4. Network Phase Out 119

7. Performance Standards 119
8. Incentives 119
9. Place of Performance 119
10. Period of Performance 119
11. Delivery Schedule 119
12. Security 119
12.1. Personnel Security 120
12.2. Email 120
12.3. Visits 120
12.4. Training and Certification 121
12.5. Common Access Card (CAC) 122
12.6. Physical Security 123
12.7. Facility Clearance 123
12.8. Protection of Sensitive and Classified Data 123
12.9. Media Sanitization and Disposal 123
12.9.1. Unclassified Media Sanitization 124
12.9.2. Classified Media Sanitization 124
Appendix A. Acronyms 126

1. CONTRACTING OFFICER REPRESENTATIVE (COR)

a) Primary COR.

Name	Douglas E. Johnson
Organization	HPCMP
Department of Defense Activity Address Code (DODAAC)	963378
Address	10501 Furnace Road, Suite 101 Lorton, VA 22079
Phone Number	703 812 8205
Fax Number	703 690 2073
E-Mail Address	doug.johnson@dren.hpc.mil

b) Alternate COR.

Name	Brett R. Evenstad
Organization	Naval Information Warfare Center (NIWC) Pacific
DODAAC	N66001
Address	53560 Hull Street, Code 55350 San Diego, CA 92152-5001
Phone Number	619 553 3737
Fax Number	619 553 5991
E-Mail Address	brett.evenstad@dren.hpc.mil

2. CONTRACT TITLE

Defense Research and Engineering Network 4 (DREN4) Contract.

3. BACKGROUND

The High Performance Computing Modernization Program (HPCMP), established in response to Congressional direction in 1992 to modernize Department of Defense (DoD) high performance computing (supercomputing) capabilities, is chartered to establish, provide, and maintain leading edge High Performance Computing (HPC) capability for scientists and engineers engaged in DoD RDT&E missions. Additional background material on the HPCMP is at https://www.hpc.mil.

The Defense Research and Engineering Network (DREN), a component of the HPCMP, provides secure high performance wide area network services in support of DoD scientists and engineers, as well as other related DoD communities and Federal agencies. All of these groups and organizations when connected to the DREN Network are the “DREN Subscribers”, a term used throughout this PWS. The networks they attach to DREN are referred to as the “Subscriber Enclave”.

3.1. DREN Evolution

DREN4 is the fifth generation of DREN. The first generation was Government owned and operated. All subsequent DREN generations have been accomplished under Indefinite Delivery/Indefinite Quantity (ID/IQ) network services contracts. The history of DREN is depicted in Figure 3.1, showing how the network services, bandwidths, and implementations have evolved over time to keep up with new technologies and increasing bandwidths.

Figure 3.1 DREN History

DREN 0 "IDREN" (1995-1997) • Government-owned • T1s and T3s • Cisco routers • Native Internet Protocol (IP) • Asynchronous Transfer Mode (ATM) test bed • Defense Information Systems Agency (DISA)-supported Network Operations Center (NOC)	**DREN 1 "DISC" (1997-2002)** • AT&T ID/IQ contract (5-year) • Cisco (IP), Fore (ATM) • OC-12 (13 x DREN 0) • ATM (native) • IP over ATM • IPv6 test bed over ATM • Vendor-provided NOC
DREN 2 "DREN II" (2002-2012) • Verizon ID/IQ contract (10-year) • Juniper routers • IPv4 and ATM over Multi-Protocol Label Switching (MPLS) • 10 Gigabits (16 x DREN 1) • IPv6 "when commercially available" • IP Security (IPsec) and VPLS [Virtual Private LAN Service] (Ethernet) added • Lightwave services • Vendor-provided NOC	**DREN 3 "DREN III" (2012-2022)** • CenturyLink ID/IQ contract (10-year) • Alcatel-Lucent-Nokia routers • 100 Gigabits (10 x DREN 2) • IPv6 with support for legacy IPv4 • Ethernet and IP Services, No ATM • Optical Services (Optical Wavelength Service, Optical Transport Network, Alien Waves) • Vendor-provided NOC

The current DREN networking service is provided by a private virtual Wide Area Network (WAN)built on a commercial communications network and provides transport services between defined sites that comprise DREN. Sites are currently specified in terms of bandwidth requirements, physical interfaces, and transport protocols.

DREN is a high performance communications network that incorporates the best capabilities of both DoD and the commercial infrastructure. DREN includes connectivity to other Research and Education (R&E) networks via private and public peering. Currently DREN comprises more than 180 sites ranging in bandwidths from 50 Megabits per second (Mbps) through 40 Gigabits per second (Gbps). DREN changes continually with the addition of new sites, changing bandwidths at existing sites, removal of existing sites, and insertion of new technology into the network.

3.2. DREN Technical Leadership

Through the many generations of DREN, DREN has been a leader in the implementation and use of advanced high performance networking technologies. For example, the DREN community was among the early users of the Advanced Research Projects Agency Network (ARPANET) and has been a leader in emerging technologies such as IPv6.

DREN4 is a significant shift from DREN III, with most of the intelligence of the network moving from the network edge to the network core. This will have multiple benefits, including:

a) network routing and other processing is done in the core at provider's locations, allowing for fewer aggregated resources and less equipment at difficult to access Government sites

b) the edge no longer requires expensive routers

c) ability to implement hop-by-hop encryption that readily aligns with the core architecture

4. OBJECTIVES

The objective of this contract is to provide state-of-the-art WAN transport and related services to support the DREN community. DREN's primary mission is to support the DoD HPC, Research and Development (R&D), Science and Technology (S&T), Test and Evaluation (T&E), Modeling and Simulation (M&S), and Acquisition Engineering (AE) communities. DREN also provides network services to other select Federal Agencies and academia. The network links the DREN community together, to supercomputing resources, and to Federal, academic and Cloud Service Provider (CSP) networks, as well as the Internet.

All activities on this contract shall comply with all standards and guidance as prescribed in the awarded contract and references therein.

It is anticipated that DREN4 will be implemented as follows:

a) Upon contract award, begin Initial Performance Capability (IPC)

b) No later than 12 months after contract award, begin execution of Comprehensive Implementation and Transition Plan (CITP)

c) No later than 24 months after contract award, complete execution of the CITP

5. SCOPE

DREN is a services contract providing high performance network and related services to the DREN Communities (as outlined above) anywhere, anytime.

5.1. DREN4 Program Objectives

Transport and service requirements for DREN4 are derived from Subscriber requirements for synthesized network environments and the need to engage in collaborative initiatives. Many DREN Subscribers 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, DREN4 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) Connectivity to CSPs

h) Special dedicated connectivity between members of a Community of Interest (COI).

i) Shorter term dedicated (virtual) connectivity builds for special projects, exercises, and demonstrations.

5.2. Continuation of DREN Services

Current DREN networking capability is provided under the DREN III Contract administered by Defense Information Technology Contracting Organization (DITCO). This procurement will enable continuation of DREN network services.

5.3. Service Locations and Duty Hours

The Contractor shall provide DREN services on a 24 hour a day, seven day a week all days of the year basis. This will be referred to in this PWS as 24x7x365. Since every calendar day is a working day, no distinction is made in this PWS between them. All reference to days indicates calendar (which is also working days). Locations supported under the current DREN contract as well as future anticipated sites are identified in the Contract Line Item Number (CLIN) Tables. Service to any listed location may or may not be ordered under this solicitation. Additional locations may be added as fully negotiated modifications to the contract. Locations can be both within and outside CONUS [Continental United States].

5.4. Synopsis of Future Network

DREN4 represents a significant change in the requirements and characteristics of the services provided and where the services will be placed in the network. Figure 5.1 outlines the key features of DREN4.

Figure 5.1

DREN 4 "DREN4" (2022-2032)

- ID/IQ contract (10-year)
- Lightweight edge with intelligent core
- Switching, routing, and computing functions
- Software Defined Networking (SDN), Network Function Virtualization(NFV), orchestration
- 400-Gigabits (4 x DREN 3)
- IPv6 with support for legacy IPv4
- Ethernet and IP Services
- Hop-by-hop encryption (i.e., Media Access Control Security (MACsec))
- No optical services
- Vendor-provided NOC

6. PERFORMANCE REQUIREMENTS

DREN4 will be a high-performance DoD WAN service, providing Layer-2 Ethernet and Layer-3 IP transport and associated services to DREN Subscribers, primarily at U.S. locations. This will incorporate most of the network characteristics of DREN III, but will evolve to include higher bandwidths, organic encryption, faster provisioning, increased resiliency, robust access to CSPs, better support for security infrastructure, added visibility and control in the core, and other features to address Subscribers needs and security threats. There will be a NOC responsible for overall network monitoring and control, along with a help desk and online support portal for Government and Subscriber interactions. The network will be accredited in accordance with Risk Management Framework (RMF) standards and policies.

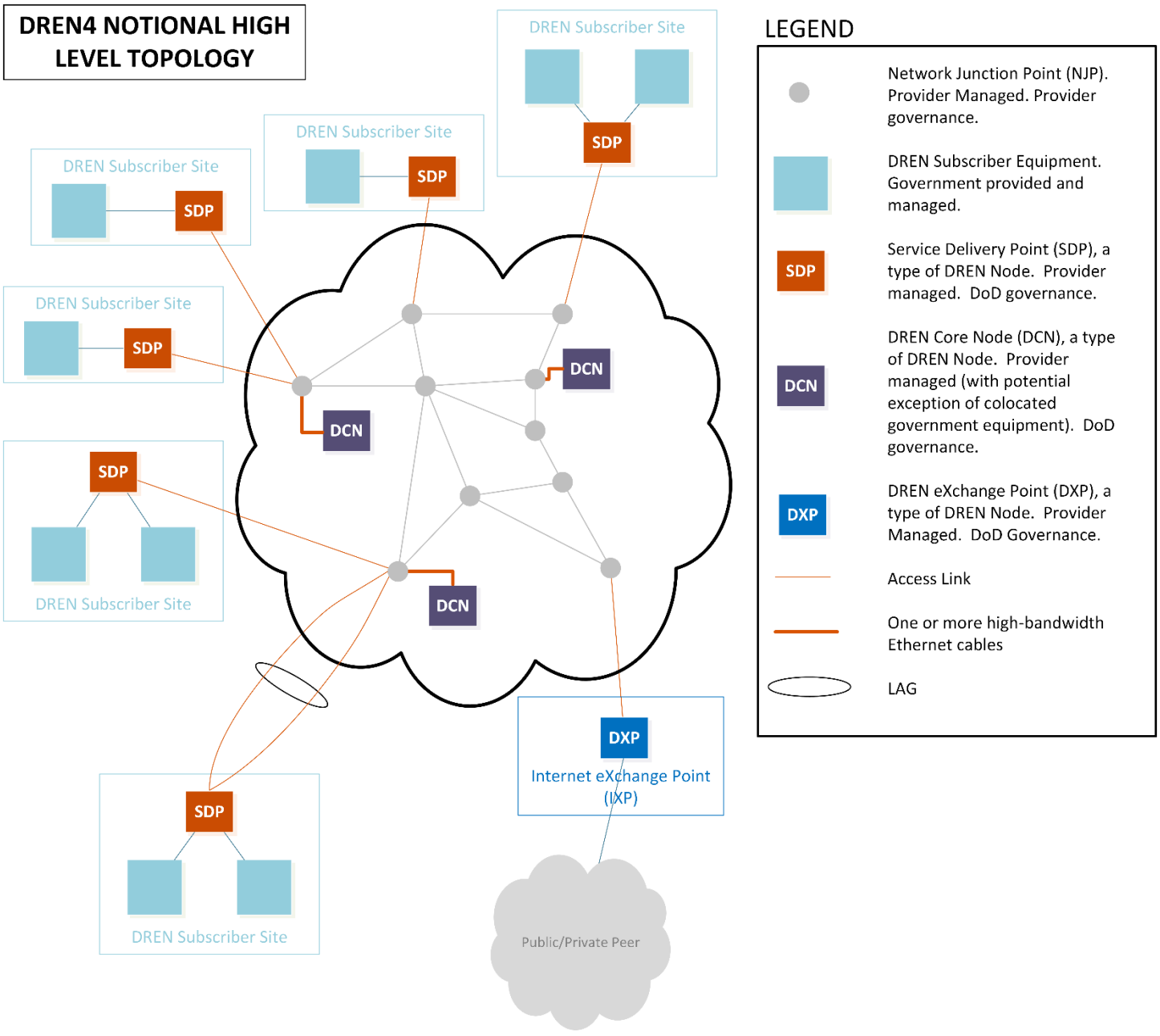
Ethernet transport will include a wide area Ethernet service, offering private Virtual Local Area Networks (VLANs) and trunks between DREN Subscribers upon request. IP transport will include full functionality for both IPv6 and legacy IPv4 protocols, with unicast, multicast, and anycast routing and addressing features. This will be instantiated as multiple independent IP networks, with some being pre-defined and others added during the life of DREN4. Router functions in the network will interconnect these networks as required using standard internal and external routing protocols and will provide peering to external networks and transit services to the full Internet. These IP and Ethernet networks will be grouped into "Collectives" (a DREN-unique term) based on governance, routing architecture, encryption, and other attributes. Interconnects between Collectives will include a Security Gateway (SG) function administered by the Government.

DREN is implemented as a private overlay network on existing commercial network infrastructure and services. In this document, the term "provider" will be used to refer to the owner or manager of the underlying network over which DREN is constructed and operated. The "provider network" is that portion of the underlying network used to implement DREN. This could also be referred to as the "provider core" or "provider backbone".

Building DREN will require the provider to connect DREN Nodes to the provider network. This connection could be implemented using fiber, a wavelength, a circuit, or other technologies, or a combination of the above, along with any associated regeneration, multiplexing, switching, or routing. In this document, these connections will be referred to as an “access link”

It is assumed that the provider network is constructed of high speed data links interconnecting major junctions where switching, routing, and other functions exist. These junctions will be termed Network Junction Points (NJPs). It is assumed that these NJPs are in provider owned and controlled facilities.

DREN4 will be comprised of physical nodes (i.e., "DREN Nodes") interconnected by provider backbone and access links. There will be three types of DREN Nodes, generally characterized by location and purpose, and named Service Delivery Point (SDP), DREN Core Node (DCN), and DREN eXchange Point (DXP).



SDPs are physically installed at Subscriber sites to deliver DREN services to the Subscribers at a given location.

DCNs are at provider facilities and are all interconnected via the provider backbone, forming a network "intelligent core". They perform switch, router, and other network functions, instantiated either physically or virtually. They will be strategically placed to minimize latency between other DREN Nodes, and will be appropriately sized to meet aggregate demands.

DXPs are installed at Internet eXchange Points (IXPs) and other locations for public and private external peering.

SDPs and DXPs will be "homed" to DCNs. All DREN Nodes will communicate primarily via MACsec enabled Ethernet paths at rates of 1G, 10G, 100G, or multiples thereof.

DREN Nodes will all include a switch function, to provide bridging of Ethernet segments, and to provide VLAN support. DREN Nodes will optionally include a router function, to provide routing between IP network segments, and to support routing protocols. These functions could be provided physically or virtually.

DREN4 performance requirements include a geographically based maximum latency between DREN Node pairs. There is also a requirement to support single-stream Transmission Control Protocol (TCP) at near line-rate, with some specific exceptions (e.g., 100G+ over large distances).

DREN4 Security requirements include the need for confidentiality and integrity using encryption over any shared infrastructure. Some DREN Subscribers will separately encrypt their data, but where this is not the case then portions (VLANs) of the access links must be encrypted. Between DCNs, certain VLANs must be encrypted across the provider backbone. MACsec is the encryption required for any of the Ethernet based connections.

A DREN SDP will be comprised of the minimum hardware necessary to meet Subscriber connection requirements, generally no more than a managed Ethernet switching function with support for MACsec encryption and enough interfaces to support the access link and all independent Subscribers at that site. IP router functions will not be needed at most SDPs, but will instead be performed at a DCN.

DXPs will require cross-connects within a facility to reach exchanges, national research and academic networks, and direct connections to CSPs.

DCNs will perform the bulk of DREN traffic processing, using physical appliances and/or virtual functions on a NFV platform, tailored to meet performance requirements for all SDPs and DXPs homed to a given DCN. DCN functionality includes encryption/decryption of access and backbone Ethernet paths, Ethernet switching, IP routing (unicast, multicast, and anycast) for both IPv6 and legacy IPv4 using internal and external routing protocols as appropriate. DCNs may also include compute and storage infrastructure to support NFV where DREN4 functions can be implemented virtually if of sufficient performance, and where unique government needs (e.g., virtual security appliances) may be implemented.

DREN4 will peer with many external networks, primarily at the DXPs, but to reach the rest of the Internet it may subscribe to Internet Transit Service (ITS) at two or more locations. The ITS locations will be at DCNs or DXPs, optimally chosen based on the provider's topology.

It is envisioned that network components and functions will have mainstream Application Programming Interfaces (APIs) that enable role-based access to programmable configuration, observation, and other SDN type functionality, which can then be orchestrated to support repeatable processes to facilitate automation

and faster provisioning and improved visibility and control. Example uses are where DREN could provision VLANs between multiple cooperating sites and optionally enable encryption, or opt-in to security controls in the core, or instantiate a service chain of security functions tailored to their enclave.

Where rapid provisioning is required (days instead of months), or where the Subscriber's need is temporary, or otherwise unique, and where performance requirements can be relaxed, the Government includes the SDP Lite (SDP-L) requirement. SDP Lite is a normal SDP except the access link is any connection of opportunity (3G, 4G, 5G, cable modem, Non-Classified IP Router Network (NIPRNet), etc.) that is available at the Subscriber site to securely tunnel traffic to a DCN, and where the site personnel perform the physical installation of the hardware and its connections. Transport performance requirements are relaxed for this situation.

6.0. Base Requirements for All Tasks

6.0.1. Hardware and Software

All of the hardware and software used in the network shall be compatible, fully interoperable, and completely support all of the features necessary to meet or exceed the requirements.

All hardware and software shall be compliant with all relevant Government guidance documents including at a minimum being on the National Information Assurance Partnership (NIAP) Product Compliant List

6.0.2. General Guidance

In all cases in the PWS where a feature, capability, or characteristic is stated as "shall…", then the Contractor shall take all necessary steps to implement that requirement.

Although the typical use of the term Subscriber is used to describe other organizations and groups with connections to DREN Nodes, for the requirements here, the HPC and DREN Program are also Subscribers when connected to the network and using DREN services.

In the DREN 4 Contract the HPC DREN program is the customer, however, any reference to Customer in this PWS shall mean both the DREN program as well as the Subscribers to the network.

References to "the Government" in this PWS shall mean Government representative(s) as designated by the DREN Program Manager through the Contracting Officer (KO).

For Deliverables, Standard Distribution shall mean one copy of the transmittal letter with the deliverable to the Contracting Officer and to the COR(s); and the Deliverable submitted and made available to the Government in the 6.5.10.2 Government Documentation Repository.

6.1. DREN Transport

DREN transport shall include the transport of layer 2 Ethernet frames and layer 3 IPv6 and legacy IPv4 packets between any DREN Nodes.

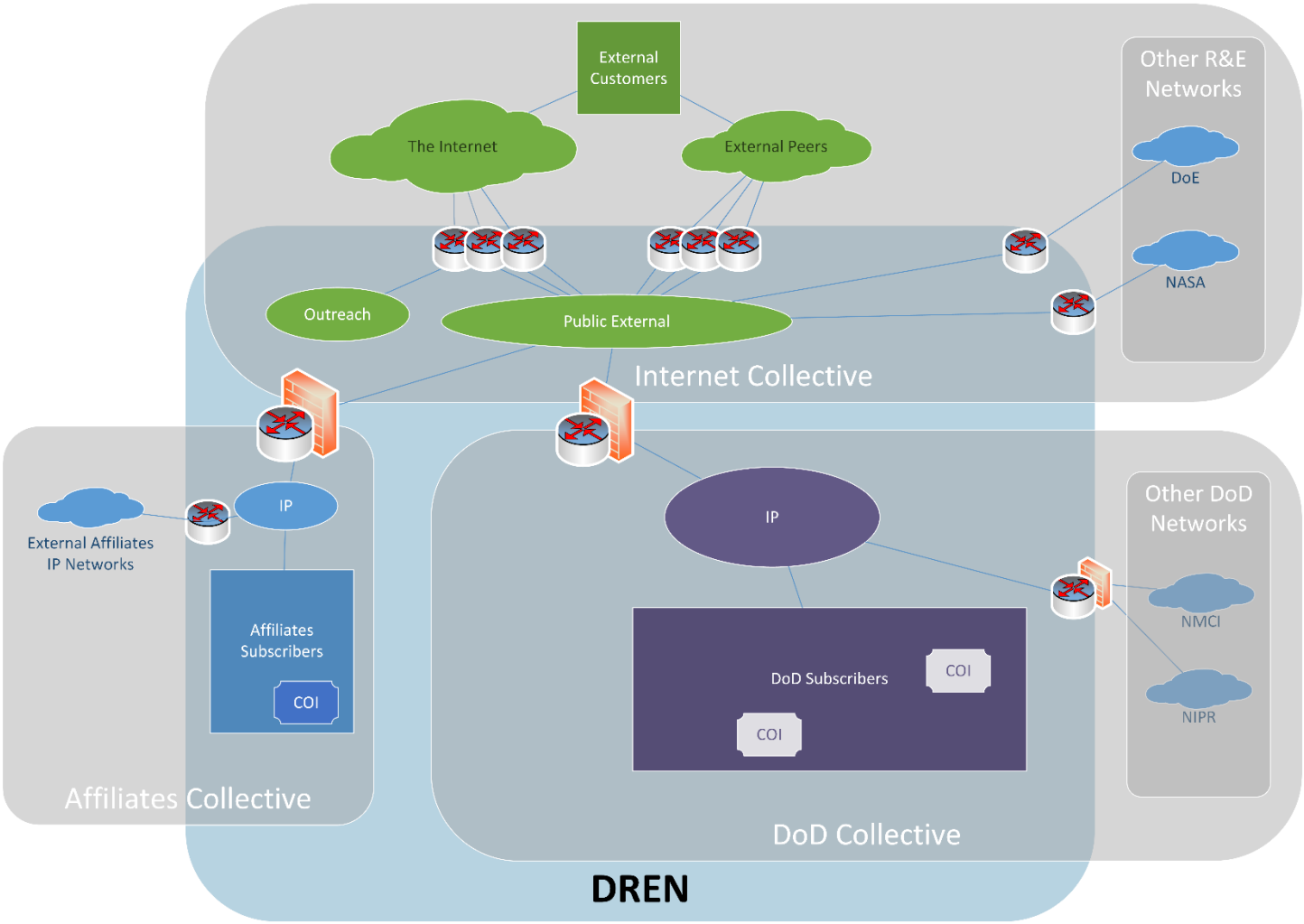
Ethernet and IP traffic transmitted between and through DREN Nodes shall be transported through the shortest path available that maintains the performance requirements, the security requirements, and other

policy characteristics. The transport requirements also include establishing connectivity to external DoD, Federal, private peers and the Internet.

6.1.0. Elements of Base Task

6.1.0.1. Collectives

DREN III introduced and defined the term Collective, a term that is unique to DREN and which is used to group networks at the macro level based on governance and routing architecture. Each of the many Layer-2 or Layer-3 networks implemented on DREN will be a member of one (and only one) of these Collectives. Collective membership is used to define how a given network must be implemented on DREN, how it connects to other networks, and how strongly it must be separated from other networks.



Governance is a primary attribute for defining Collectives. Governance acknowledges the established policies for how networks must be built, secured, accredited, and operated. Networks within a given Collective can interconnect with one another with minimal restrictions. Network interconnections between Collectives must traverse border controls that may be very restrictive.

Routing and switching architecture is another attribute of Collectives. The network and routing topology, External Gateway Protocol (EGP), Interior Gateway Protocol (IGP), and other factors will differ depending on the Collective.

There are currently three Collectives: DoD Collective, Internet Collective, and Affiliates Collective. The DoD Collective includes all networks that carry intra-DoD traffic. The Internet Collective includes the networks that directly connect to the Internet through public and private peering. The Affiliates Collective includes networks supporting other (non-DoD) Federal Agencies.

The DoD Collective is governed primarily by DoD 8500.01 and related policies, and its member networks must be protected and accredited in accordance with DoD 8510.01. These networks connect directly to DREN Subscribers and to other external DoD networks (e.g., NIPRNet). These networks require strong separation and protection from underlying commercial networks and from networks in other Collectives, generally through use of encryption technology. These networks must not cross a border to other Collectives, unless they do so via an approved SG. The routing architecture in the DoD Collective focuses on the optimization of intra-DoD traffic routing, and best exit through an SG.

The Internet Collective is governed through Best Current Practices (BCPs) (as defined by the Internet Engineering Task Force (IETF), North America Network Operator's Group (NANOG), and other associations), and through bilateral peering agreements with other Internet Service Providers (ISPs). Routing architecture in the Internet Collective focuses on internal and external metrics for optimizing traffic flows to and from the Internet.

The Affiliates Collective is governed by the requirements of the Agencies that its member networks support. They fall outside the scope of DoD governance, yet need protection from the open Internet. DREN will provide separation from other networks, but specific boundary protection infrastructure such as Managed Trusted Internet Protocol Service (MTIPS) is outside the scope of DREN.

6.1.0.2. Performance

The ability to transfer data between DREN Nodes shall be possible at the DREN Node rate mutually available between the two DREN Nodes.

The Contractor shall engineer and install transport capacity sufficient to support all DREN Nodes simultaneously transmitting at the peak data rates specified by the Government. The Contractor shall expand transport capacity should subsequent modifications or additions to DREN Nodes on the network exceed the available transport capacity.

Each DREN Node's transport functions shall operate with sufficient independence such that:

- The ability to provide concurrent transport between other DREN Nodes shall not have any reduction in performance.
- Any testing shall not reduce transport performance for all DREN Nodes not under test.
- The Contractor shall design DREN Nodes and Transport such that individual capabilities and functions can be added, modified, or eliminated without reducing the performance of other existing capabilities and functions.

6.1.0.3. Buffering

Sufficient buffering shall be provided wherever switching and routing takes place to sustain high performance TCP flows. This means that each transport device (physical or virtual) shall support the allocation of a Bandwidth Delay Product (BDP) worth of buffering to a single flow. For example, an 80 ms Round Trip Time (RTT) requires buffering of 10MB for 1G interfaces and 100MB for 10G interfaces.

6.1.1. Ethernet

The DREN4 network shall transport Ethernet frames between and through DREN Nodes. All delivered services (e.g., IP) will be transported over this Ethernet layer. The network shall support switching, encryption, layers of 802.1Q tagging, and multicast.

6.1.1.1. Switching

The DREN4 network shall support bridging and switching functions. The bridging architecture and infrastructure shall support automatic and dynamic:

a) shortest transport paths with adequate capability/capacity

b) loop prevention

c) separation and protection at appropriate levels (e.g., National Institute of Standards and Technology (NIST) Security controls, Collective governance)

d) traffic distribution

e) quality of service preservation, prioritization, and pathing

f) topology changes and traffic redistribution around failures

g) Ethernet broadcast and multicast distribution that provides shortest delay and minimizes resource consumption

h) Protection from floods (rate issues) and storms (amplification issues)

Basic STP [Spanning Tree Protocol] is not sufficient to meet the above requirements. Other technologies such as Shortest Path Bridging (SPB), TRansparent Interconnection of Lots of Links (TRILL), Equal-Cost Multi-Path (ECMP), or Ethernet Virtual Private Network (EVPN) could be configured to meet or exceed the requirements. The requirements are not written to constrain the offeror to one of these standards or one vendor implementation. The Government will specify which Switch Functions are edge (not used for transit traffic between other Nodes); all others are middle (used for transit). The contractor shall deploy and configure Switch Functions to ensure edge Switch Functions are ineligible for transit traffic.

6.1.1.2. Multicast

The network shall support Ethernet broadcast and multicast. The implementation must minimize how much broadcast and multicast traffic is replicated over a given path for each VLAN. Bifurcation shall occur within the DCNs (the DREN core), not at the edge (SDP/DXP).

To properly transport IPv6 multicast Ethernet frames, all layer 2 switching functions in the network shall fully support MLD snooping and MLDv2. To properly transport IPv4 multicast Ethernet frames, all layer 2 switching functions in the network shall fully support IGMP snooping and IGMPv3.

6.1.1.3. Ethernet Quality of Service (QOS)

End to end Quality of Service (QoS) controls shall be implemented across the DREN Network. At the Ethernet layer, 802.1p priority levels shall be supported. Although marking of any of the eight values shall be used to appropriately order and route the frame, it is understood that Network Control (NC) at the transport level is reserved for other than DREN Subscriber traffic. The marking of NC must be preserved but transported as if marked at the next highest level. At all elements of switching function, the priority shall be used to appropriately order and route the frames.

If Ethernet transport is carried over other protocols the original priorities must be preserved, and mapped to the transport prioritization mechanism so that its prioritization is acted upon at every higher transport function.

6.1.1.4. VLAN

The Ethernet frames will be delivered over 802.1Q "VLANs" at the interface on the DREN Node. Each VLAN, as specified by the Government, shall be configured to transport to the given set of DREN Nodes. The network shall support thousands 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.

6.1.1.5. Encryption

The Ethernet transport shall support encryption. All Ethernet traffic shall be encrypted unless specifically indicated otherwise by the Government. This encryption shall be implemented using MACsec hop-by-hop encryption between Switch Functions that are physically and logically protected for processing non-encrypted DREN traffic. The encryption can be inherent to the switching function or can be separately applied but shall meet all PWS requirements including transport performance (6.1.0.2) and Ethernet transport requirements (6.1.1). The MACsec header overhead is a component of the minimum frame transport size (6.1.1.6). For traffic specifically designated as not requiring encryption (e.g., already encrypted, test traffic), the solution shall allow for bypass VLANs. In the provider's core, these VLANs shall bypass the hop-by-hop MACsec imposed path through DCNs and be switched directly to the destination DREN Node(s).

6.1.1.6. Frame Size

The network shall support transport of an Ethernet frame size of at least 9154 bytes end to end (i.e., between any DREN interfaces). This minimum requirement does not include overhead due to network topology (SPB, TRILL, etc.), or outer transport header(s). This frame size is selected to support a double-tagged 9100 bytes service frame with MACsec encryption and normal Ethernet headers. The 9100 bytes service frame is to

support for example a 9000 byte IP packet that is a separately double-tagged MACsec encrypted frame. All elements of transport shall support at least this frame size.

6.1.1.7. Ethernet Resiliency

The transport bridging protocol shall be sufficient to properly forward frames even in the presence of a failed path, a failed DREN Node (other than the endpoints), or any degraded element that would normally be part of the Ethernet transport. Failures shall result in a new optimized topology that bypasses the degraded or failed element. All requirements for transport shall still be met for all functioning aspects of the network elements.

All DREN Nodes shall have a MACsec and bridging relationship with two or more DCNs. The path used shall be to the nearest DCN. In the event of a DCN failure, the forwarding shall occur to the next nearest DCN.

6.1.2. Internet Protocol (IP) Transport

DREN4 must include an IP Transport Service that routes and delivers IP packets natively end-to-end between and through DREN Nodes. Multiple independent IP networks will be in DREN, some are predefined and others that will be implemented during the life of the contract as needed.

Each IP network must support unicast routing, and may require IP multicast and/or anycast routing as well. Router Functions in the network may route IP packets between the various IP networks as required, and between Subscriber networks and other external peers.

References to "IP" imply both IPv6 and IPv4 protocols.

IP Transport Services are delivered over Ethernet connections to DREN Subscribers or peers.

All network addressing (prefixes) in use on DREN will be provided by the Government, with the exception of the Outreach service (6.1.2.11.2).

6.1.2.1. IPv6

The primary IP protocol is IP version 6 (IPv6). All IP functionality and services shall fully support IPv6. Some IP networks (6.1.2.8 Multiple IP networks) may require IPv4 support as well, in a "dual stack" configuration, while others will be IPv6-only (e.g., the management networks).

All systems, software, and equipment supporting the network and its services shall support IPv6 capabilities (including features, performance, and security) in an equivalent or better way than IPv4. The Contractor shall not deploy any systems, software, or equipment on DREN that does not meet this requirement. The Contractor shall configure all network systems, software, and equipment to utilize IPv6 in an equivalent or better way than IPv4. The Contractor shall have a corporate commitment to IPv6.

6.1.2.2. IPv4

IP version 4 (IPv4) is considered the "legacy IP protocol", and shall be supported on IP networks as needed, but shall not be in use on certain IP networks such as the management networks (6.1.2.8.5 Management Networks). Where IPv4 is not in use, interfaces of devices connected to the IP network shall not have IPv4

addresses configured on the interface in order to ensure that no IPv4 traffic is generated and so these devices will not respond to any IPv4 traffic that might unintentionally exist on such networks.

6.1.2.3. IP Maximum Transmission Unit (MTU)

The network shall accept, transport, and deliver packets with an IP MTU of at least 9000 bytes, without fragmentation. The Contractor shall configure the IP MTU of any Subscriber facing interface to 9000 bytes unless otherwise directed by the Government. IP MTU refers to the entire IP packet, including the IP header, but not any encapsulating headers or trailers.

Path MTU Discovery shall be supported on all DREN network paths. This includes the proper generation and delivery of Internet Control Message Protocol (ICMP) messages for Packet Too Big (IPv6) and Fragmentation Needed (IPv4).

6.1.2.4. Unicast

The DREN4 networks shall support the delivery of unicast traffic in all aspects of the IP Service.

6.1.2.5. Multicast

The Contractor shall provide a robust native IPv6 and IPv4 multicast capability both within the DREN community and between DREN and external networks in all phases of the contract. The IP Multicast capability shall include multicast route, source, traffic exchange, and efficient tree management. The capability shall meet the same bandwidth and latency requirements as IP Unicast capability for the multicast path taken. The IP Multicast capability shall support at a minimum Any Source Multicast (ASM), Source Specific Multicast (SSM), Protocol Independent Multicast-Sparse-Mode (PIM-SM), Multicast Source Discovery Protocol (MSDP) Internet Group Management Protocol (IGMP) v3, and Multicast Listener Discovery (MLD) v2. The IP Multicast infrastructure shall perform efficient bifurcation away from the site and be configured to work with underlying IP routing and Ethernet switching. A rendezvous point (RP) topology shall be designed and implemented for each IP network with sufficient capacity for performance requirements and redundancy to support availability requirements. The IP Multicast capability shall support security and control mechanisms based on best current practices for IP Multicast and shall include the ability to place blocks at external peering, internal peering, or Subscriber interfaces including Border Bootstrap Router (BSR) limit, PIM block, and scoping limits by direction of the Government.

6.1.2.6. Anycast

Anycast, or one-to-one-of-many routing, shall be supported. When multiple hosts share the same destination address, the network shall route traffic destined for that address to the nearest one. The pairing of a given source to its nearest anycast destination shall be stable. Any given pair shall only change when failure of the anycast host or the path to that host occurs. The Contractor shall implement anycast as part of the normal Border Gateway Protocol (BGP) routing. In addition, for IPv6, the ability to configure "host routes" as discussed in Request for Comments (RFC) 4291 shall be supported.

6.1.2.7. IP Quality of Service (QoS)

End to end QoS controls shall be implemented across DREN. At the IP layer, the network shall support RFC 2475 DiffServ, including the Expedited Forwarding (EF) and Assured Forwarding (AF) Per-Hop Behaviors (PHB). If carried over other protocols at layers below IP, different IP classes of service shall be mapped to lower layer QoS mechanisms and acted upon (e.g. using PBB-TE [Traffic Engineering], Differential Services (DiffServ) aware MPLS (MPLS-TE / MPLS-TP [Transport Profile]), or similar, depending on the implementation).

Where routing occurs, the Contractor shall ensure that the IP layer accepts packets that have already been tagged with DiffServ Code Point (DSCP) values and apply the corresponding DiffServ PHB's to them. Where routing occurs, the Contractor shall ensure that IP packets can be initially tagged or retagged with DSCP values based on combinations of protocol, ports, DSCP values, and source and destination addresses.

6.1.2.8. Multiple IP networks

DREN4 shall support multiple IP networks. Each IP network shall be isolated and independent of any other network. IP networks will be interconnected as needed through Router Functions in the network. IP networks will be grouped into "Collectives" (6.1.0.1 Collectives).

The current predefined IP networks include "Public External", "DoD Only", and "Non-DoD Access", which shall be implemented as defined below.

6.1.2.8.1. Public External (PX) IP Network

The PX IP network resides within the Internet collective and exists in support of peering with all external non-DoD networks. The network will carry the full default-free Internet routing table and is the transit network for all DREN connectivity to the Internet and non-DoD private peers. The Contractor shall follow all Internet BCPs. The PX traffic does not require encryption. Currently, this network operates as part of autonomous system number (ASN) 668.

6.1.2.8.2. DoD Only (DO) IP Network

The DO IP network resides in the DoD Collective and exists to route IP traffic for DoD Subscribers and other DoD networks. It has internal peering relationships with DREN Subscribers, and external peering relationships with other DoD networks (e.g., NIPRnet, Navy/Marine Corps Internet (NMCI)), and carries ONLY DoD routes (over 15,000 routes). Currently, this network operates as ASN 333.

6.1.2.8.3. Non-DoD Access (ND) Network

The ND network resides in the DoD collective and exists to route IP traffic from DoD Subscribers to the other Collectives including the Internet. Its only function is to provide IP transport between DoD Subscriber networks and the SGs (6.1.2.9.5) which provide access to other Collectives. It shall not provide transport between DoD Subscribers directly. Currently, this network together with PX operates as ASN 668.

6.1.2.8.4. Extended DMZ (ED) Network

The ED IP Network resides in the DoD Collective and exists to support systems and servers that provide public reachable services to the Internet.

6.1.2.8.5. Management Networks

Management Networks reside in the DoD collective and exist to support management of network devices and systems, and are generally implemented as flat isolated networks to meet security requirements. These networks shall use only IPv6, and shall not carry any IPv4 traffic. All network devices and systems shall be fully functional in an IPv6-only environment, and all management services and protocols must fully support IPv6.

6.1.2.9. IP Routing

IP networks are interconnected using physical or virtual routers. These routers provide IP routing and forwarding functionality as a component of DREN Nodes, primarily DCNs. These routers receive IP packets on one network interface and forward them out a different network interface at high speed based on routing information learned from neighboring devices using various routing protocols. Routers may filter or modify the IP packets in any number of ways before processing them.

6.1.2.9.1. Best Current Practices

IP networks and routers shall perform IP routing and forwarding functions following Internet BCPs and conventions, and operate standard gateway protocols for the exchange of routing information.

6.1.2.9.2. Routing Protocols

Industry standard IP routing protocols shall be employed to distribute routing information between all IP routers in the network.

An IGP, either Open Shortest Path First (OSPF) or Intermediate System – Intermediate System (IS-IS), shall be used for routing within DREN. The IGP shall carry all DREN infrastructure routes. The IGP shall carry sufficient metrics for every link and path to enable routing decisions based on relative distance, hop count, and other network conditions. The Contractor shall permit Government managed devices to participate in the IGP.

An EGP, including MultiProtocol Border Gateway Protocol (MBGP), shall carry the external routing information for all external networks and for DREN Subscriber networks. The EGP shall support Multi-Exit-Discriminators (MEDs) from Subscribers and external peers to steer traffic between autonomous systems (ASs).

The IP routing protocols shall support authentication in compliance with relevant security controls (6.3 Security).

6.1.2.9.3. Peering

In the context of this PWS, "Peering" refers to exchanging routing information with other networks via an EGP. DREN seeks to have rich external peering. DREN will establish connectivity to external networks where there

is benefit to DREN and its Subscribers. DREN does not operate as a Tier-1 ISP. For connectivity to any other external network, the Government may use the 6.1.2.11 Internet Transit Service (ITS).

The Government intends to have the PX IP network peer with other research and educational networks, with other Federal Agency networks, and with other networks that are determined to be beneficial to DREN. The Government primarily intends to connect external peers at the DXPs, but the Contractor shall support physical connections to external peers at any DREN Node.

The Government intends to have the DO IP network peer with other external DoD networks using MBGP, including NIPRNet at three locations.

Internal peering with DREN Subscriber networks will exist via connections at SDPs. The Contractor shall support Subscribers:

a) being able to logically connect to one or more IP networks

b) using static IP routing on no more than one of their IP connections to DREN

c) using MBGP to exchange routing information and to make routing decisions

A very common Subscriber configuration will include IP connections to both the DO and ND networks, will use MBGP to exchange routing information with the DO network, and will use either static or MBGP routing with the ND network. The Government will provide direction to the Contractor on how to configure each Subscriber's IP routing.

In the very rare situation where a Subscriber requires access to the full Internet routing table, the Contractor shall support an MBGP connection to a Router Function that carries all Internet routes (e.g., the PX network).

Separate MBGP connections shall be used for IPv6 routes and IPv4 routes. Within a given address family, exchange of unicast routes shall be implemented, while exchange of multicast routes shall be implemented where directed by the Government. This applies to both external and internal peering.

6.1.2.9.4. Architecture

The Contractor shall implement the IP networks and associated routing infrastructure to deliver IP packets via optimal paths between source and destination. The Contractor shall ensure intra-DREN IP traffic is routed via the shortest path through intermediate nodes (e.g., DCNs) from the point of DREN network ingress to the point of egress.

While the Government may order a Router Function at any DREN Node, in general this will be only at the DCNs. Most DCNs will include Router Functions. SDPs and DXPs will rarely include (if ever) a Router or other separate Functions, leaving only the Switch Function.

DREN Subscriber routers connect through their SDP to nearby DCNs over Ethernet VLANs. In the same way, external peering routers connect through a DXP to nearby DCNs. IP transport is established through these connections to DCNs that have a Routing Function, called "IP homing". IP homing is to the nearest DCN, and optional backup IP homing is to the next nearest DCN. In the majority of cases, there are no intermediate Ethernet-only DCNs in the IP homing path, so in these cases the DCNs are called "Primary DCN" and "Secondary DCN".

Where the nearest Ethernet-only DCN is different from the IP homing DCN, then references to the DCNs should be qualified with Ethernet or IP, as in "Primary IP DCN" or "Secondary IP DCN".

IP homing will include static or MBGP routing relationships with these IP DCNs.

When IP homing is to both Primary and Secondary DCNs, the implementation shall support either symmetric (active/standby) or asymmetric (active/active) routing on a case-by-case basis, as specified by the Government. The Contractor shall provide mechanisms and protocols to support detection of failures of the primary DCN and initiate failover to the secondary DCN, and to revert to the primary DCN once it has been restored.

When establishing external peering with nationwide networks, multiple connections to a given external network will be established if available at multiple DXPs. A minimum of three such connections per external network is the Government's intent, for regionalization of traffic and for resiliency. The Contractor shall research and recommend DXP locations and peers available at DXPs to support the Government's intent wherever possible. Traffic routing to or from the Internet via PX and external peers shall be optimized for low latency or other Government-specified parameters (e.g., tuned with internal and external metrics, using "hot potato" routing).

IP traffic through a network can be asymmetric, in that a flow's traffic in one direction may take a different path than that flow's traffic in the opposite direction. Stateful devices such as firewalls need flows through them to be symmetric. The Government intends to insert stateful devices in some traffic flows through some DCNs; therefore, such traffic would need to be made symmetric. The Contractor shall support routing methods for any given IP network to force symmetry through the Router Functions where needed, as specified by the Government.

6.1.2.9.5. Security Gateways (SGs)

SGs are the components of the network that are used to implement security controls between Collectives. These components include physical or virtual functions provided and maintained by the Government, and are located at DCNs. These functions may be provided through physical and/or virtual appliances in the DCN. The Government envisions instantiation of approximately six SGs in the network, regionally distributed.

6.1.2.9.6. Route Filtering

DREN Router Functions shall be able to filter IP routes based on various attributes and logic. There shall be the ability to accept, deny, or modify any specific route, based on static information such as a given IP prefix, or on dynamic information.

The following attributes shall be supported, at a minimum, for route policy matching and modification:

- prefix-length
- AS-path
- community
- local-preference
- MED
- area

6.1.2.10. Controls, Policies, and Filtering

Routers shall perform various filtering and traffic control functions. Routers must include the following control mechanisms, for use as required and directed by the Government:

a) Traditional stateless Access Control List (ACL) to filter traffic based on source address, destination address, protocol, source port, destination port, and other attributes. See (6.5.2 Change Request Provisioning) on how the Government will communicate ACLs.

b) RFC 3704 (BCP 84) "Ingress Filtering for Multihomed Networks". The unicast Reverse Path Forwarding (uRPF) mechanisms described in this RFC shall be used on all Subscriber-facing interfaces to accomplish this protection.

c) RFC 5635 "Remotely Triggered Black Hole (RTBH) with uRPF", and related RFCs, for protection against Distributed Denial of Service (DDoS)attacks.

d) RFC 5575 and associated later standards for BGP Flowspec.

e) BOGON and Martian filtering.

   1) The IPv6 prefixes specified in the Cymru Bogon list currently at https://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt shall not be routed. The IPv4 prefixes specified in the Cymru Bogon list currently at https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt shall not be routed. The prefixes shall be updated dynamically or manually at least once a day.

   2) The IPv6 prefixes specified in the Routing Arbiter DataBase (RADB) Martian list currently at https://www.radb.net/query?keywords=fltr-martian6 shall not be routed. The IPv4 prefixes specified in the RADB Martian list currently at https://www.radb.net/query?keywords=fltr-martian shall not be routed. The prefixes shall be updated dynamically or manually at least once a month.

f) Modified forwarding actions:

   1) Sink: Traffic identified by the Government (e.g., malicious traffic) will be sent to a designated dead-end monitoring device managed by the Government.

   2) Scrub: Traffic of a questionable nature or of particular interest to the Government shall be routed to device(s) managed by the Government to perform inspection. This traffic will then be passed either unaffected, repaired, filtered, or blocked. The resulting packets will then need to be routed to the original destination.

   3) Redirect: Traffic designated by the Government to be blocked or otherwise undeliverable shall be routed to a device managed by Government. 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 Government.

g) Traffic shaping mechanisms must be provided to perform rate limiting of particular IP flows or sets of IP flows, applied at a router interface.

6.1.2.11. Internet Transit Service (ITS) (Separately Orderable)

The Contractor shall provide IP (IPv6 and IPv4, unicast and multicast) connectivity to the full Internet via a Tier-1 ISP. The Contractor shall configure ITS as an external peer to PX (6.1.2.9.3 Peering, 6.1.2.8.1 Public External (PX) IP Network), unless otherwise directed by the Government. This service shall be available at a minimum of five DCNs or DXPs, geographically dispersed, based on the optimal network topology of the service provider.

6.1.2.11.1. Full Internet Transit

The Contractor shall provide IP transit from DREN Networks to any part of the global Internet. This provides DREN connectivity to networks that are not otherwise reachable via other external peering, or during failure of other external peers.

6.1.2.11.2. Outreach

Outreach is an IP network that resides in the Internet collective. It provides commercial Internet-only access. It is a non-attributable (not associated with US Government) service to the Internet from any DREN node. The Outreach IP external peering/routing shall occur at the same location where the ITS is provided.

6.1.2.11.2.1. Outreach Peering and Routing

The Contractor shall:

a) Provide the following Outreach Service routable Commercial ISP IPv6 and IPv4 address space allocations per Internet Transit Service that is ordered:
   1) A minimum of a /24 of IPv4 address space
   2) A minimum of a /48 of IPv6 address space

b) Provide the following Outreach Peering routable Commercial ISP IPv6 and IPv4 address space allocations per Internet Transit Service that is ordered:
   1) A minimum of a /28 of IPv4 address space
   2) A minimum of a /64 of IPv6 address space

c) Delegate the in-addr.arpa and ip6.arpa zones for the Outreach Service prefixes to Government identified Domain Name System (DNS) servers

d) Ensure that all allocated prefixes are not associated with and not attributable to the US Government (including the Internet Assigned Numbers Authority (IANA) registrations).

e) Accept routes for these Outreach Service prefixes in a private ASN that shall be advertised to the Internet in the Commercial ISP's ASN.

f) Ensure that any prefixes, public ASN(s), and DNS entries are appropriately registered, advertised, and used without Government identification.

g) Ensure that the AS Path for these prefixes shall not contain any ASN associated with DREN or the US Government.

The Government will manage the routing for Outreach (with the provided Outreach Service prefixes). The Contractor shall support peering using BGP at the ITS locations between Outreach and the Commercial ISP. The Outreach Peering prefixes will be used for interface addresses on the segment between Outreach and the Commercial ISP. This peering shall be logically or physically separate from any other IP Peering at the ITS location. Outreach may advertise all or part of any of the IPv6 and IPv4 Outreach Service prefixes at all of the Outreach peering points.

6.1.2.11.2.2. Outreach Transport

Transport for Outreach will occur across the DREN Ethernet Transport (6.1.1). The Contractor shall provide transport for Outreach that is logically or physically separate from the DREN4 DoD accreditation boundary. Provisioning of Outreach ports and VLANs will follow the normal Change Request process.

6.1.3. Transport Performance

A defining characteristic of DREN is its ability to support very high bandwidth single stream TCP flows. It is well known that the throughput of TCP is proportional to $\frac{\text{MTU}}{\text{RTT}*\sqrt{loss}}$

Therefore, large MTU, minimal RTT, and extremely low packet loss are all requirements of this PWS.

6.1.3.1. Latency

Latency on DREN (measured by RTT) shall be minimized both for TCP performance discussed in (6.1.3 Transport Performance) and because of real-time test and simulation work. To ensure a richly connected core architecture, the RTT between all pairs of DREN Nodes shall not exceed 0.02 times the great-circle distance in kilometers between the DREN Nodes plus 20 ms:

$$RTT \leq 0.02 * km + 20\,ms$$

For example, an SDP in San Diego, CA and an SDP in Albuquerque, NM are separated by a great circle distance of 1016 km. The RTT over the network path between them shall not exceed 40.3 ms.

This latency limit shall be met for Layer 2 (Ethernet) and Layer 3 (IPv6 and IPv4) paths.

The topology and infrastructure of the network shall be constructed to meet this requirement.

The Contractor shall meet the latency requirement between any two DREN Nodes. The requirement applies pairwise over the provider network (i.e., not through intermediate DREN Nodes).

If the median RTT (i.e., 50th percentile) between a given pair of DREN Nodes exceeds the formula, that pair has failed to meet the latency requirement.

If more than five pairs from any DREN Node fail to meet the requirement, that node fails to meet the PWS latency requirement.

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.1.3.1 Latency	Latency Formula	For all DREN Nodes, no more than 5 pairs exceed Latency Formula requirements.	Government review of contractor developed Latency Report.	See Node Credits (6.5.7.2 and 6.5.8.2)

6.1.3.2. Jitter

Jitter on DREN shall never exceed 0.1 milliseconds. This applies to frame/packet streams between any pair of DREN Nodes. Jitter refers to the delay variation between consecutive frames/packets as defined in International Telecommunications Union (ITU) Y.1540 and Y.1541.

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.1.3.2 Jitter	Jitter Measurement	Jitter between all pairs of DREN Nodes is less than 0.1 milliseconds.	Government review of jitter as reported in the 6.5.10.1.3 Data Dashboard	See Node Credits (6.5.7.2 and 6.5.8.2)

6.1.3.3. Loss

Low packet loss is essential to DREN performance. The Contractor shall monitor packet loss on all DREN paths. At no time shall the packet loss rate on any DREN path exceed 0.01%. The exception to this requirement is congestion loss on access links caused by high levels of Government offered traffic (over subscription). The Contractor shall notify the Government of any access links that are frequently oversubscribed.

To achieve high speed TCP flows over anything other than a small distance, packet loss must be significantly less than this 0.01% loss requirement ($\frac{\text{MTU}}{\text{RTT}*\sqrt{\text{loss}}}$). For example TCP flow with RTT of 80 ms, MTU of 9000 and throughput of 10 Gbps, the packet loss rate cannot exceed 10^{-8}, which equates to a bit error rate of 10^{-12}.

While loss that is congestion induced can occur (e.g., on access links), the core networks supporting DREN have to be nearly lossless.

For these reasons, sufficiently low loss on DREN shall be demonstrated by the performance testing of TCP throughput (6.1.3.6.2 Pairwise TCP Test).

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.1.3.3 Loss	Loss Measurement	Loss on all DREN paths is less than 0.01%.	Government review of loss as reported in the 6.5.10.1.3 Data Dashboard	See Node Credits (6.5.7.2 and 6.5.8.2)

6.1.3.4. Throughput

High end-to-end throughput over DREN is essential. Every path on DREN shall provide wire speed data transfer at all times including both single stream and aggregate flows. The core network shall have sufficient capacity that all DREN nodes can transmit and receive at wire speed simultaneously. Wire speed is defined as the raw bits-per-second rate of the individual interfaces minus any encapsulation and header overhead. At no time shall the Contractor's encapsulation and header overhead consume more than 5% of the bandwidth of any ordered DREN port or line rate.

All pairs of DREN Nodes shall be capable of sustained transfers between them at the lesser of their two DREN Node Line rates. For example, between a 1Gbps DREN Node and a 10Gbps DREN Node, a transfer of 1Gbps shall be possible.

When Link Aggregation Groups (LAGs) (6.2.0.3 DREN Node Line Rate) are used to provide DREN Node access links, the single stream performance is limited by the size of each member of the aggregated link.

6.1.3.5. DCN Placement

Transport performance may be impacted by the quantity, capacity, and placement of DCNs. In particular, latency may increase due to additional hops and increased distances through DCNs, and bandwidth could be constrained by oversubscription at a DCN. The Government seeks to minimize the performance impact of DCNs by a cost-effective optimization of their quantity, location and capacity (e.g., line rate, functions).

The Contractor shall

a) provide information and advice to support the Government’s ordering choices

b) use an optimizing methodology to propose the quantity, capacity, and placement of DCNs such that

   1) end to end latency is minimized

   2) sufficient aggregate capacities are available

c) prepare one or more current geographical map(s) in a format developed by the Contractor with Government input showing existing state (DCN Placement Current Map(s)) with:

   1) the DREN Nodes and the underlying network with all of the NJPs (6 Performance Requirements and 6.2.0.2.2 DREN Core Node (DCN))

   2) the placement of existing DCNs at those points

   3) the Line Rates at all DREN Node locations

   4) the interconnections from SDP and DXP nodes to the NJP(s)

   5) the mesh of interconnections between DCNs

   6) any other pertinent data representable on the map(s)

d) prepare a DCN Placement Current Report in a format developed by the Contractor with Government input showing existing state with:

   1) a spreadsheet representation of:

A) List of all SDPs and DXPs showing the NJP where the access link ends

B) List of all NJPs showing if in use by DREN, and the Latitude and Longitude.

C) The interconnections, latencies and bandwidths between all of the NJPs

2) any other data not representable in map form in an appropriate format

3) discussion of the optimizing methodology including

A) A description of the methodology and any changes to it since last report.

B) the measure and calculated components of that methodology

C) recommendations to the Government

The Contractor shall use current state measured values and locations to produce the DCN Placement current Map and DCN Placement Current Report.

The Contractor shall use a combination of current data and the output of the network optimization methodology and produce DCN Placement Proposed Map(s) and DCN Placement Proposed Report in the same format as the DCN Current Map(s) and Report. In this DCN Placement Proposed Report, the Contractor shall include discussion and rationale of any proposed changes (e.g., additions, deletions, relocations, capacity increases and decreases).

Upon award, the Government will provide feedback to tune the Contractors methodology and calculations. After proposed maps are included in the IPC plan (during the IPC and CITP phases), the Current Map(s) and Report shall be prepared monthly and include Proposed Map(s) and Report if warranted. After CITP, Map(s) and Report(s) shall be updated annually, at any time the DREN Nodes or Contractors underlying network is significantly changed, and when requested by the Government.

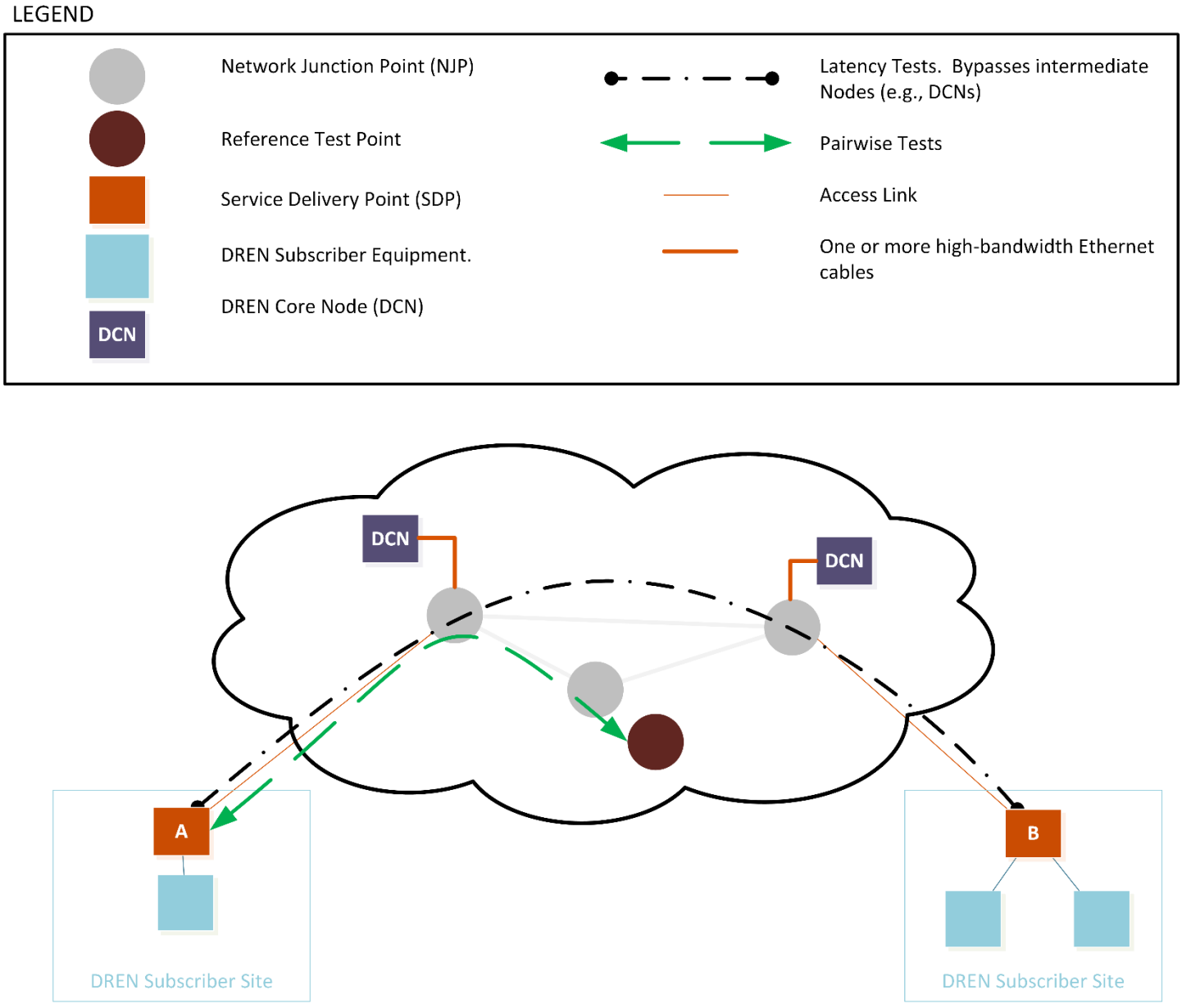
PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.1.3.5	DCN Placement Current Map(s)	Contractor-Determined Format	15 days after Government request		Standard Distribution (6.0.2)	Monthly through CITP, Annually after CITP, after any significant changes, and upon Government Request
	DCN Placement Current Report					
	DCN Placement Proposed Map(s)					
	DCN Placement Proposed Report					

6.1.3.6. Measurement and Testing

Figure 6.1 DREN Measurement and Testing Diagram shows the measurement and testing environment of DREN. The majority of DREN traffic is expected to flow over encrypted paths through DCNs. The presence of DCNs in the path might affect performance (e.g., latency and throughput).

It shall be possible to perform performance tests over non-encrypted paths that bypass the DCNs. The Government will consider that such tests are sufficient to demonstrate that transport performance requirements are being met. All of the specific tests in this Element shall be performed over a non-encrypted Node-to-Node Layer 2 path. Acceptance tests shall not reduce the service performance of any accepted DREN Nodes. The Contractor shall provide reference test point(s) on the network (independent of all ordered DREN Nodes). These reference test points shall be used to perform the pairwise acceptance tests. These reference test points are not separately priced.

Figure 6.1 DREN Measurement and Testing Diagram



6.1.3.6.1. Latency Test

RTT is commonly measured using ICMP echo packets (i.e., "ping"). The provider shall measure RTT between all pairs of DREN nodes at least once every five minutes and report results to the Government monthly no later than the 15th of each month. The report shall identify which node pairs fail the latency requirement (6.1.3.1 Latency).

Latency measurements shall be performed by an ICMPv6 ping or an Ethernet method to effect the measure. To perform a ping either the switch function would need to support a separately IP addressed test interface (independent of the management interface which must communicate over the encrypted path) or an additional test component added at a DREN Node. To perform Ethernet based testing, either the Y.1731, 802.1ag, or a similar (and at least as capable) method shall be used.

If end-to-end measurement is not possible, piecewise measurements shall be added together.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.1.3.6.1	Latency Report	Contractor-Determined Format	15th of each month		Standard Distribution (6.0.2)	Monthly

6.1.3.6.2. Pairwise TCP Test

Sufficiently low packet loss shall be demonstrated by TCP running at 80% of wire speed between a given pair of sites. For example, on a 10 Gbps path, at least eight Gbps of TCP user payload shall be demonstrated. In testing tools such as nuttcp and iPerf, the user payload rate is the number reported. The tests shall be conducted with a commercial off-the-shelf TCP stack, e.g., on a Linux system, not via simulated TCP test traffic. The test shall be IPv6, bi-directional, and run for at least 20 minutes.

For some combinations of high bandwidth and long RTT paths 80% of wire speed is not possible, due to the 1GB maximum TCP window size. For such cases, if the BDP of a tested path exceeds 500MB, then N parallel TCP tests can be run, where N is determined by dividing the BDP by 500 and rounding up. The aggregate throughput for the N parallel streams shall sum to 80% of the aggregate speed or better.

If the DREN Node access link is provisioned over an aggregated link (6.2.0.3 DREN Node Line Rate); the Contractor shall test every individual member of that aggregation while all members are up. Each member of that aggregated link must perform at 80% of wire speed of that member.

The pairwise TCP test from a given node shall be conducted to one or more destinations of equal or greater Line Rate. The RTT of the test path shall be at least 20 ms. Remote loopbacks are acceptable in tests. This test shall be performed as part of DREN Node acceptance. The Government may request a retest at any time. Typically, this will be requested when problems are suspected, or at times when a significant change to the DREN Node or its connectivity occurs.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.1.3.6.2	On Demand Pairwise TCP Test Report	Contractor-Determined Format	15 days after Government request		Standard Distribution (6.0.2)	Upon Government Request
Acceptance tests will include this Pairwise TCP Test and results are delivered under 6.5.14 Acceptance Testing						

6.1.3.6.3. Aggregate TCP Test

The Contractor shall perform an aggregate TCP throughput test to demonstrate core network performance meets the requirements. Pairwise TCP tests described in (6.1.3.6.2 Pairwise TCP Test) shall be performed simultaneously between all pairs of nodes to achieve this demonstration.

The aggregate TCP throughput in and out of each DREN Node shall be at least 80% of that node's Line Rate, and should be distributed evenly between all pairs.

After the initial aggregate test in IPC, the Contractor shall perform additional aggregate tests on all or a portion of the DREN Nodes when requested by the Government. Typically, this will be requested when problems are suspected, or at times when a significant change to the network occurs.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.1.3.6.3	On Demand Aggregate TCP Test Report	Contractor-Determined Format	15 days after Government request		Standard Distribution (6.0.2)	Upon Government Request
IPC tests will include this Aggregate TCP Test and results are delivered under 6.6.1.1.6 IPC Demonstration Report (IPCDR)						

6.1.3.6.4. Pairwise Throughput Test

The testing of DREN Node Line Rate at 95% throughput shall be demonstrated Node pairwise using method(s) from ITU-T Y.1564 or equivalent. This testing shall be performed at acceptance (6.5.14 Acceptance Testing) and any time after that requested by the Government.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.1.3.6.4	On Demand Pairwise Throughput Test Report	Contractor-Determined Format	15 days after Government request		Standard Distribution (6.0.2)	Upon Government Request
Acceptance tests will include this Pairwise Throughput Test and results are delivered under 6.5.14 Acceptance Testing						

6.1.3.6.5. Aggregate Throughput Test

The Contractor shall perform an aggregate throughput test to demonstrate core network capacity meets the requirements. Pairwise tests described in (6.1.3.6.4 Pairwise Throughput Test) shall be performed simultaneously between all pairs of nodes to achieve this demonstration.

The aggregate throughput in and out of each DREN Node shall be at least 95% of that node's Node Line Rate, and should be distributed evenly between all pairs.

After the initial test in IPC, the Contractor shall perform additional tests on all or a portion of the DREN Nodes when requested by the Government. Typically, this will be requested when problems are suspected, or at times when a significant change to the network occurs.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.1.3.6.5	On Demand Aggregate Throughput Test Report	Contractor-Determined Format	15 days after Government request		Standard Distribution (6.0.2)	Upon Government Request
IPC tests will include this Aggregate Throughput Test and results are delivered under 6.6.1.1.6 IPC Demonstration Report (IPCDR)						

6.1.3.7. Degradation/Outage

If any of the transport performance requirements (e.g., latency, loss, jitter, or throughput) are not met from a given DREN Node, an outage will be declared for that node until full performance has been restored. The Government may choose to declare a node in a degraded state, e.g., when latency or loss exceed requirements but communication is still usable.

Once a node is declared degraded, it will not be used to penalize any additional nodes. For example, a high RTT on a degraded node will not cause other nodes to fail their pairwise latency requirement.

6.2. DREN Node

A DREN Node is a set of Contractor provided components (hardware and/or software) to deliver the ordered services at a specified location.

The DREN Node is the interface between Government equipment and the Contractor provided services.

Each DREN Node shall operate independently of other DREN Nodes but in a manner that complies with requirements for interoperability and network functions.

The Contractor's service and implementation of DREN Nodes shall transfer data between and among simultaneously connected DREN Nodes in such a way that:

a) The ability to provide concurrent transport services to other active DREN Nodes shall not be negatively impacted.

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

c) The ability to utilize the DREN Node capabilities that implement requirements shall be maintained; and testing of these capabilities at a DREN Node shall not reduce the service performance provided via any other DREN Node.

d) DREN Node Services shall be able to transfer data limited only by the interface on the node and the DREN Node's Line Rate.

The Contractor shall design DREN Nodes such that individual DREN Node Functions and Services can be added or eliminated without affecting other existing interfaces or functions, or services regardless of type.

The Contractor shall manage active DREN Nodes in a manner that permits the Government to utilize the DREN Node performance capabilities at all times.

The Contractor shall engineer and provision all switch function ports and cabling, and any other services needed to provide the functions described in these Subtasks that the Government orders.

The Contractor shall implement components in DREN Nodes that support the 6.1.0.3 Buffering requirement.

Some of the subtasks/elements/sub-elements of this task apply to every DREN Node while others are separately orderable and only apply to DREN Nodes where they are ordered. The separately orderable items can be not ordered, ordered once, or ordered multiple times for placement on any DREN Node.

6.2.0. Elements of Base Task

6.2.0.1. Government Data and Access Requirements

The Government will own and operate independent data collection and analysis systems for all DREN4 configurations, performance data, and log information. This is in addition to any data collection and analysis required of or performed by the Contractor.

6.2.0.1.1. Flow

A real-time copy of all flow data (sFlow [Sampled Flow], IPFIX[IP Flow Information eXport], and/or NetFlow [Network Flows]) from all DREN4 devices, physical or virtual, shall be transmitted to a minimum of two government specified IPv6 addresses.

6.2.0.1.2. Log

A real-time copy of all log information from all DREN4 devices, physical or virtual, shall be transmitted in its original raw format via syslog [System Logging] protocol to a minimum of two government specified IPv6 addresses.

6.2.0.1.3. Simple Network Management Protocol (SNMP)

The Contractor shall provide direct SNMPv3 read-only access to information (including configuration and utilization) on all managed DREN4 devices, physical or virtual.

The Contractor shall configure SNMPv3 in AuthPriv SHA [Secure Hash Algorithm]/AES [Advanced Encryption Standard] mode using Government provided authentication and encryption credentials for Government

access. A minimum of two Government provided IPv6 addresses shall be permitted to perform SNMPv3 queries to all DREN4 devices.

It is likely that publish/subscribe systems such as Streaming Telemetry will augment or replace SNMP and even BGP route reading in the future. The Contractor may be requested to provide a 6.4.3.1 Technology Insertion Proposal (TIP) to implement this or a similar technology in the future.

6.2.0.1.4. BGP

The Contractor shall provide BGP access from a minimum of two Government specified IPv6 addresses (and additionally two IPv4 addresses if the MBGP session cannot communicate both IPv6 and IPv4 routes in the single IPv6 BGP session). These BGP peerings shall be configured to export all routes and import none (i.e., read-only). The Contractor shall provide access to any devices that contain BGP routing tables upon Government request.

6.2.0.1.5. Government Access to Network Components

At the request of the Government, the Contractor shall provide designated Government personnel read-only access to the CLI [Command Line Interface], Web Graphical User Interface (GUI), or similar access method to any DREN4 network device and/or their centralized controller(s) within the DREN4 accreditation boundary for the purpose of reviewing configuration information and obtaining current state. The Government will access the network components using IPv6. If authentication to these devices requires a hardware token, the Contractor shall provide the required tokens to the Government.

6.2.0.2. DREN Node Types

There are three types of DREN Nodes.

a) Service Delivery Point (SDP) which has three subtypes:
   1) SDP Standard (SDP-S)
   2) SDP Lite (SDP-L)
   3) SDP Hybrid (SDP-H)

b) DREN Core Node (DCN)

c) DREN eXchange Point (DXP)

6.2.0.2.1. Service Delivery Point (SDP)

The SDP will typically be located at DREN4 Subscriber premise locations. The SDP will provide the link to the DREN Core, and switching functions (6.2.1 Switch Function (One included)). There are three variations of SDP. The first is the SDP Standard (SDP-S) which meets the full requirements of a DREN Node. Second is the SDP Lite (SDP-L) which has unique connectivity to the Core and relaxed requirements (6.2.9 SDP Lite (SDP-L), 6.2.10 Tunnel Termination Point (TTP) (Separately Orderable). It is anticipated that a third type that is a hybrid of these two will exist in the future, SDP Hybrid (SDP-H) (6.4.3.1.6 Hybrid SDP).

6.2.0.2.2. DREN Core Node (DCN)

The DCN will primarily be located at the Contractor's locations (NJPs). The Government will order the placement of DCNs, which will be coordinated with the Contractor post-award. The DCN will provide flexible routing, encryption, and security for the core of DREN4. The DCN will provide services for one or more SDPs.

6.2.0.2.3. DREN eXchange Point (DXP)

The DXP will primarily be located at IXPs and other peering locations. The DXP provides services to support external peering (e.g., with private peers, internet transit services, cloud providers).

6.2.0.3. DREN Node Line Rate

Each DREN Node shall have the capability to support two-way full duplex aggregate data transfer rates to the rest of the network for all data traffic managed by that DREN Node through all interfaces. The data rates for a DREN Node will be specified by the Government from the data rates listed in Table 6.1. These rates apply to all user traffic at a DREN Node, regardless of protocol or DREN Node Service at the originating or terminating DREN Node.

The rates specified are aligned with existing Ethernet interface speeds. The access link connecting the DREN Node must support data transfer at a rate equal to or greater than the line rates specified in Table 6.1:

Table 6.1 Line Rates

1 Gbps
N x 1 Gbps
10 Gbps
N x 10 Gbps
100 Gbps
N x 100 Gbps
400 Gbps
N x 400 Gbps

The “N x” Line Rates may be implemented using a single access link of sufficient rate, or with multiple access links that are aggregated, concatenated, or FlexE [Flexible Ethernet] bonded together.

When "N x" Line Rates are implemented by aggregation:

a) Ethernet Frames shall be assignable to a specific member of a LAG using attributes of the frames including at least those defined in (6.2.1 Switch Function (One included)-implement L2 based filtering)

b) IP streams shall be able to be specifically assigned to a member of a LAG using differentiated aspects of the IP packet that correspond to hashed factors from the set available which meets or exceeds (6.1.2.10 Controls, Policies, and Filtering)

c) performance testing of each member of the LAG requires the ability to map a TCP test stream to individual members of a LAG (Hashing to LAG members is vendor dependent, so the details of this mapping for testing purposes will be determined after award)

The DREN Node shall provide at least 95% of the line rate at all times. This requirement shall be demonstrated by running the (6.1.3.6.4 Pairwise Throughput Test).

The DREN Node line rate shall apply to all user data transmitted through an SDP, excluding protocol overhead needed for framing, routing, or encryption of the user data to the destination endpoint.

The Contractor shall engineer and install connectivity from the Provider Backbone to each DREN Node to support the Line Rate ordered for that DREN Node.

6.2.0.4. Physical Security at DCN and DXP Locations

The Contractor shall install all DREN Node equipment at the DCN and DXP Locations such that it meets the physical security requirements specified in 12.6 Physical Security.

6.2.1. Switch Function (One included)

The Contractor shall provide a Switch Function with every ordered DREN Node that meets or exceeds the requirements in this subtask. The Switch Function shall support all of the Ethernet transport services defined in 6.1.1 Ethernet. In addition, the Switch Function shall:

a) add VLAN tag(s) to tagged or untagged frames

b) remove VLAN tag(s) from tagged frames

c) perform VLAN translation

d) prioritize frames based on (6.1.2.7 IP Quality of Service (QoS)) marking if no Ethernet QoS marking is on the frame

e) aggregation/bonding of multiple ports

f) implement L2 based filtering

1) support the following selectors

A) source Media Access Control (MAC) address(es)

B) destination MAC address(es)

C) VLAN Tag(s)

2) implement the following actions

A) permit

B) drop

C) rate shape

D) set/modify priority

g) mirror traffic to Government designated ports, with the following capabilities

1) replicate bidirectional traffic from one or more physical port(s) to one output port

2) replicate traffic on one or more port(s) in each direction (ingress and egress) to separate output ports based on the direction (i.e., ingress traffic to one output port, and egress traffic to a different output port)

3) add an 802.1Q VLAN tag on replicated/mirrored traffic

4) not drop any frames unless the aggregate of mirrored traffic exceeds the bandwidth of the output port

h) support Provider Backbone Bridging (PBB)

i) support auto negotiation on all port and modules including flow control (e.g. PAUSE frames, Priority-based Flow Control (PFC))

j) support enabling and disabling negotiated flow control on a per port basis

6.2.1.1. Ports (Separately Orderable)

The Switch Function shall support multiple ports of various speeds and types per Table 6.2 Ports, for interconnecting Subscriber equipment. Each Switch Function shall be non-blocking between all of its ports. The Contractor shall maintain the size of each Switch Function to accommodate the number and speed of the ports ordered.

Table 6.2 Ports

1G Copper
1G Pluggable
10G Copper
10G Pluggable
100G Pluggable
400G Pluggable

100G Pluggable Ports will only be ordered at DREN Nodes with at least a 10 Gbps Line Rate. 400G Pluggable Ports will only be ordered at DREN Nodes with a 400 Gbps Line Rate.

6.2.1.2. Modules (Separately Orderable)

The Contractor shall support the Modules from (Table 6.3 Modules). The modules shall be made part of a pool available for placement and/or relocation to any Switch Function Port of matching speed, in any DREN Node, at the Government's direction. A Switch Function port only moves if the Switch Function and/or DREN Node are moved.

Table 6.3 Modules

1000BASE-T
1000BASE-SX
1000BASE-LX
1000BASE-EX
1000BASE-ZX
10GBASE-T
10GBASE-SR
10GBASE-LR
100GBASE-SR4
100GBASE-LR4
400GBASE-SR8

6.2.1.3. Interconnections

The Switch Function and its interconnections to other Functions may be provided physically or virtually, as long as it meets the PWS requirements. The Switch Function included with every DREN Node interconnects with the DREN WAN, and to any additional Functions (Switch, Router, Firewall, and/or Compute) at that Node. These interconnections are not separately ordered or specified, but are integral parts of the individual Functions. These interconnects shall not limit the throughput or performance of the ordered services on a DREN Node in any way.

6.2.1.4. Additional Switch Functions (Separately Orderable)

Each ordered DREN Node comes with one Switch Function (6.2.1 Switch Function (One included)). The Government may order additional (optional) Switch Functions for any DREN Node. These may be implemented as separate physical devices, partitions of an existing device, or as virtual instances. Additional Switch Functions shall operate independently from all other Switch Functions. All Switch Functions shall be managed by the Contractor unless the Government chooses to assume control of an optional Switch Function. The Government may either choose to manage optional Switch Functions directly, or via an Orchestrator ordered by the Government. In the case of Government control, the Contractor will provide in-band management access to the Switch Function for Government use.

If a Switch Function requires connectivity to any existing Switch Functions, and these are not provided virtually, the Government will order ports and/or modules on both Switch Functions and direct the Contractor to interconnect them along with the Additional Switch Function.

6.2.2. Router Function (Separately Orderable)

One or more optional Router Functions may be ordered for any DREN Node. The Contractor shall either deliver the Router Function using a physical router, a virtual router, or by enabling Layer-3 support in the Switch Function. In this Router Function, the Contractor shall deliver IP router functionality to support all the

IP routing requirements specified in 6.1.2 Internet Protocol (IP) Transport. In general, DCNs will include a Router Function, but SDPs and DXPs will not.

Sizing of the Router Function is primarily driven by the number of routes supported but also by the forwarding throughput. The Contractor shall meet the requirements of each size (Small, Medium, and Large) in Table 6.4 Router Function Sizes. The Plus size options include larger routing and forwarding tables to support full Internet routes.

Table 6.4 Router Function Sizes

Size	Small	Medium	Medium-Plus	Large	Large-Plus
Throughput	10 Gbps	100 Gbps	100 Gbps	400 Gbps	400 Gbps
Routing Table Size	30,000 routes	30,000 routes	2,000,000 routes	30,000 routes	2,000,000 routes
Forwarding Table Size	20,000 entries	20,000 entries	1,000,000 entries	20,000 entries	1,000,000 entries

6.2.3. Firewall Function (Separately Orderable)

An optional stateful firewall function may be ordered at any DREN Node. This "Firewall Function" will handle larger and/or more complex filtering that is beyond the offered capabilities of the Switch and Router Functions. The Government anticipates potentially using this Firewall Function at DCNs both as a Security Gateway component and to serve Subscribers.

The Contractor shall implement the Firewall Function with the following capabilities:

a) large numbers of rules based on the five tuple (source and destination address, source and destination port, and protocol)

   1) any tuple can be a singleton, a set, or 'any'

   2) port definitions shall also permit ranges (e.g., 0-65535)

   3) address definitions shall also permit subnet specifications (e.g., 192.168.10.0/28) and geographic/country designations

b) stateful filtering

c) perform filtering at the throughput ordered

Firewall Functions can be ordered in three sizes with the minimum capabilities shown in Table 6.5 Firewall Function Sizes.

Table 6.5 Firewall Function Sizes

Size	Small	Medium	Large
Rules	5,000	10,000	40,000
Throughput	10 Gbps in+out	40 Gbps in+out	100 Gbps in+out
New sessions per second	50,000	100,000	250,000
Total sessions	3,000,000	6,000,000	20,000,000

A Firewall Function could be a physical or virtual device. The Firewall Function shall be managed by the Contractor, unless managed through Orchestration (6.2.5 Orchestration). Rulesets and updates to those rules will be provided by the Government (6.3.3 Network Protections, 6.3.4 Initial Boundary Protection Deployment, 6.3.5 INFOCON/CPCON Changes).

6.2.4. Compute Function (Separately Orderable)

The Contractor shall provide a Compute Function with all necessary hardware, switch ports added to the device providing the Switching Function, and interconnections. The Compute Function will be used by the Government for purposes such as NFV, DREN Joint Sensor (DJS), and DREN Active Measurement Program (DAMP). The Compute Function shall be capable of running virtual systems of variable core, memory and storage characteristics. The Contractor shall provide mechanisms for the government to instantiate new virtual systems by service request and/or by direct control e.g., via a web-based interface.

In the following specifications, a core shall be a real, non-hyperthreaded, individual processor within a CPU [Central Processing Unit]. The Contractor shall provide all but the cores necessary for management of the virtualization environment (up to two maximum) for use with Government virtual systems. Each of the following specifications is the minimum required.

All Systems shall have:

a) Intel x86_64 architecture with Kaby Lake or later series processors running at 2.4 GHz or faster

b) TPM [Trusted Platform Module] 2.0

c) provide the government ability to load a system from the following image types:

   1) ISO [International Organization for Standardization 9660] image

   2) OVA [Open Virtualization Appliance]/OVF [Open Virtualization Format]/VMDK [Virtual Machine DisK]

   3) QCOW2 [QEMU [Quick Emulator] Copy On Write version 2]

d) storage of at least 10K RPM spinning disk or SSD [Solid State Drive]

e) storage transfer rates of at least 800MB/s

f) minimum of 2666MT/s memory speed

g) network performance of line rate access to the physical interfaces prescribed

6.2.4.1. Generic Compute Function

A Virtual Machine (VM) is a guest system running on the compute function. A virtual network interface is the representation of a Network Interface Card (NIC) to the VM. The “Host” is the underlying system (e.g., hypervisor) supporting the VMs.

The Contractor shall provide the Government with console access to the VMs. At a minimum, this includes serial console.

The Contractor shall implement the Generic Compute Function to support the following mappings:

a) one or more physical interface(s) out of the interfaces (see Connectivity in Table 6.6 Generic Compute Platform Sizes and Requirements) to a VM's virtual network interface(s)

b) one or more VLANs on a physical interface or lagged multiple interfaces to one or more VM's virtual network interfaces

c) one or more VLANs between virtual network interfaces of multiple VMs

All mapped connections shall be switched as needed within the Host.

The Contractor shall configure the mapping and switching from Government submitted service requests (6.5.2 Change Request Provisioning)

Table 6.6 Generic Compute Platform Sizes and Requirements

Size	Small	Medium	Large
Cores	14	28	56
Memory	128GB	512GB	1TB
Storage	4TB	16TB	64TB
Connectivity (interfaces)	4x1G	2x10G	1x100G

6.2.4.2. DAMP Compute Function

A DAMP has unique requirements above the generic compute function. The Contractor shall provide an independent bare metal system with at least one PCIe3 [Peripheral Component Interconnect express Generation 3] slot that is at least a half-height, half-length slot for the Government to install a commercial off the shelf board. The Contractor shall provide remote graphical and serial console for the platform (e.g., IPMI [Intelligent Platform Management Interface], iDRAC [Integrated Dell Remote Access Controller], iLO [Integrated Lights-Out]) via its network connectivity to a Government specified VLAN. The government shall have complete control of the bare metal system (e.g., to configure storage partitions and load OS images and data, upgrade system firmware).

Table 6.7 DAMP Compute Sizes and Requirements

Size	DAMP-Small	DAMP-Medium	DAMP-Large
Cores	16 (single socket)	16 (single socket)	16 (single socket)
Memory:	32GB	64GB	64GB
Storage	1TB	1TB	1TB
Connectivity	1x1G 1 remote console	1x10G 1 remote console	1x100G 1 remote console

6.2.4.3. DJS Compute Function

A DJS has unique requirements above the generic compute function. The Contractor shall provide this as an independent bare metal system with the network interface(s) specified in Table 6.8 DJS Compute Sizes and Requirements. The mirror interfaces shall be interconnected to the mirror (6.2.1-a)) feeds from the switching function. The storage shall be located internal to the chassis and connected by direct bus attached storage. The Contractor shall provide remote graphical and serial console for the platform (e.g., IPMI, iDRAC, iLO) via its network connectivity to a Government specified VLAN. The government shall have complete control of the bare metal system (e.g., to configure storage partitions and load OS images and data, upgrade system firmware).

Table 6.8 DJS Compute Sizes and Requirements

Size	DJS-Small	DJS-Medium	DJS-Large
Cores	14	28	56
Memory	128GB	512GB	1TB
Storage	4TB	16TB	64TB
Connectivity	2x1GE (mirror) 1X1GE 1 remote console	1x10GE (mirror) 2x1GE 1 remote console	1X100G (mirror) 1X10GE 1 remote console

6.2.5. Orchestration

Orchestration involves programmatic configuration and control of multiple physical and/or virtual networking functions. It allows for high level "intents" and service chains to be implemented without manual configuration of individual components.

DREN Node Functions (Switch, Router, Compute, and Firewall) shall support interfaces that allow their control by an orchestration system in addition to all other required capabilities. The Government will apply control ranging from simple configuration control to full NFV Infrastructure (NFVI) management.

For an orchestrated Switch, or Router Function, the control shall include that its configuration can be created, read, updated, and deleted (CRUD) under software control using one or more of the following open industry standard protocols: NETCONF [Network Configuration Protocol], RESTCONF [REpresentational State Transfer Configuration], OpenFlow, or OVSDB [Open Virtual Switch DataBase]. This control includes the manipulation of flow forwarding match-action tables.

For an orchestrated Firewall Function, the Contractor shall provide an open API for device configuration and observation, as well as firewall ruleset(s)/rule(s) additions, modifications and deletions.

For an orchestrated Compute Function, the Contractor shall provide an open API for creating, deleting, interconnecting, and managing multiple virtual machine and/or container instances and their associated networks (virtual and/or physical).

For any devices utilizing NETCONF or RESTCONF, full YANG [Yet Another Next Generation] models for those devices shall be provided to the Government.

6.2.5.1. Orchestrator

The Government may order one or more Orchestrator instances. Each Orchestrator instance will control a collection of one or more DREN Node Functions, designated by the Government. The Government will directly control those designated Functions via a GUI and/or API provided by the Orchestrator. The Orchestrator may be physical or virtual. A partition of the Contractor's DREN Orchestration system (if any) may meet this requirement if sufficient isolation from other partition(s) is possible and required control can be given to the Government.

The Orchestrator shall provide a GUI that enables the Government to view and control the orchestrated infrastructure. For example with OpenStack, the GUI is Horizon. Equivalent GUI functionality shall be provided for other implementations. The Orchestrator shall provide an API compatible with the APIs used by AWS, OpenStack, and CloudStack. The Orchestrator shall accept templates that define the instantiation of service chains that are compatible with OpenStack (HEAT) and/or AWS (CloudFormation).

6.2.6. Internet Peering and Transit

Some DREN IP networks require connectivity to the global Internet. Connections are established through private or public peering (6.1.2.9.3 Peering) between the PX network and specific external networks. Such connections are primarily established at DXPs, but could be established at any DREN Node. If the collection of peers does not provide transit to the full Internet, 6.1.2.11 Internet Transit Service (ITS) may be ordered to provide full Internet reachability, using the same peering mechanisms as other private peers.

The Contractor shall establish physical and peering connectivity to external networks as specified throughout this PWS.

The Government will collaborate with the Contractor to determine available options and then designate where DREN will connect to external networks.

6.2.6.1. Private Peering

DREN Nodes shall support physical connectivity to other networks, and a DCN or other DREN Node with Router Function shall support the associated routing for peering. Cross-connects to external networks at DXPs will be ordered by the Government as needed. The Government will monitor traffic on these connections using the switch function mirroring capability (6.2.1-g) mirror traffic to Government designated ports, with the following capabilities) and/or passive taps (6.2.8 Passive Tap) installed on any cross-connect.

6.2.6.1.1. Colocation and Cross connects at DXP locations

6.2.6.1.1.1. Colocation

DXPs will generally be located in fee-for-service commercial facilities. The Government will order colocation services, cross-connects, and touch labor, as necessary to support DXPs at these locations. The Contractor shall in turn obtain these services from the colocation provider or other parties as appropriate for that facility. The Contractor shall ensure any ordered items and services are sufficient to meet both the Contractor's needs and the requirements of this PWS.

6.2.6.1.2. Cross-Connects

The Contractor shall provide cross-connects between DXPs and neighboring external network infrastructure as specified by the Government or in Letters of Authorization (LOAs) from that external network operator. Either LOAs will be obtained by the Government, or the Contractor shall obtain an LOA on behalf of the Government.

In general, these cross-connects will be fiber or copper connections between the DXP and an interface on the external network that the Contractor shall obtain through arrangements with the co-location facility where the DXP is located. The Contractor shall install any necessary patch cables between the patch panel where the cross-connect is terminated and the DXP interface. The Contractor shall coordinate with the external network operator as appropriate, to complete their end of the connection, to test the access link for proper operation, and to configure the DXP interface to be compatible with the external network interface.

6.2.7. Rack Space (separately orderable)

When ordered, the Contractor shall provide all necessary hardware; power; and Heating, Ventilation and Air Conditioning (HVAC) to supply a Rack Space capability for the Government to mount any of its own rack mountable hardware and supplemental equipment. The Government may order Rack Space at DCNs and possibly DXPs, but not at SDPs.

For each unit ordered at a DREN Node the Contractor shall provide an EIA[Electronics Industry Association]-310 19" 4-post rack with a minimum internal rack unit height dimension of 73.5 contiguous inches (42 Rack Units (U)). The rack space shall have physical security requirements as specified in 12.6 Physical Security. The entire rack space (42U) shall be fully usable by the Government without any obstructions (e.g., power units, cables, rack hardware). The rack shall have a minimum of 38" unobstructed space between the front and rear door or other boundaries for racked equipment and cables extending from the front and rear of that equipment. The vertical rack rails shall be fully adjustable to Government selected distance from the front and rear of the rack.

For each unit ordered the Contractor shall provide two power feeds of 208-250V 30A conditioned power with NEMA [National Electrical Manufacturers Association] L6-30R Outlets within three feet of the top rear of the rack space. The rack shall be able to accommodate Government installed full height vertical PDUs [Power Distribution Units] at the rear of the rack space.

The rack space shall be fully ventilated in both the front and rear faces/doors. HVAC cooling shall be provided at the front face of the rack and the exhaust heat removed from the rear of the rack. Each rack space shall be

provided with a minimum 45000 British Thermal Unit (BTU)/hr. heat removal. The input temperature shall be no higher than 24˚C with a relative humidity no higher than 55%.

The Government may exercise the power upgrade option to add two additional 208-250V 30A power feeds as above to a rack. This option also requires the contractor to add additional HVAC (if needed) of 45000 BTU/hr. heat removal to the minimum.

The Contractor shall give Government approved individual's access to the rack space 24 hours a day, seven days a week with 24-hour advance notification. In addition, the Contractor shall provide up to five individuals that the Government will designate access to the rack space 24 hours a day, seven days a week without any advance notification. The Contractor shall provide this access including all necessary credentialing to those designated individuals within seven days of notification by the Government. The Contractor shall execute and ensure all processes necessary to accomplish access at both Contractor facilities and other facilities where DCN and DXP type DREN Nodes exist.

Pricing shall be inclusive of all applicable charges including space charges; access charges; power charges; HVAC charges; and all labor to implement, provision and maintain the rack space.

All of the rack spaces shall be directly adjacent to the DREN Node rack with direct wire access between them.

6.2.8. Passive Tap (separately orderable)

When ordered, the Contractor shall provide an in-line passive tap service for any optical network connection at any DREN Node. The Contractor shall implement the service and connect the tap to the optical network connection and the tap monitoring interface to an LC interface on co-located Government monitoring equipment, as specified by the Government. The passive tap service shall support optical types of Multi-Mode (MM) and Single-Mode (SM).

6.2.9. SDP Lite (SDP-L)

The Contractor shall provide an alternative version of an SDP. SDP-L is similar to a SDP-S except there is no Contractor-provided access link, no on-site installation nor support by the Contractor, and relaxed performance requirements.

The MACsec-encrypted access link is replaced by encrypted (e.g., IPsec) tunnels. The tunnels are created over any "connection of opportunity" (e.g., 3G, 4G, 5G, cable modem, satellite, NIPRNet) available at the Subscriber site to securely tunnel traffic to DREN via nearby DCNs with a Tunnel Termination Point (TTP) (6.2.10 Tunnel Termination Point (TTP) (Separately Orderable)). Local site personnel will perform installation of the SDP-L equipment at the site.

There are multiple situations where SDP-L may be appropriate for certain Subscribers. These include rapid service provisioning to meet urgent requirements, interim service while awaiting provisioning of standard access links, service delivery to very low-end sites with minimal requirements, support of embedded personnel at non-DREN sites, temporary service for meetings and disaster recovery service.

The Contractor does not provide nor operate the access link for SDP-L. Standard DREN performance requirements that are dependent on the access link will not apply but shall still be measured and reported.

The Contractor shall use these measurements to assist the Government and the Subscriber in the maintenance of the link to DREN and achieving the best effort level of performance. Since no access link is required, SDP-L is a location independent CLIN.

The Contractor shall support rapid provisioning of SDP-L. The SDP-L hardware components shall be pre-provisioned and delivered to the site within four days of order. It shall be delivered with clear "quick start" instructions for site personnel to install the SDP-L and bring it online in coordination with the NOC. The NOC shall:

a) gather the specifics of the connection of opportunity (e.g., DHCP [Dynamic Host Control Protocol], static IP)

b) configure the tunnel endpoint at the TTPs

c) verify tunnel connectivity

d) logically extend the specified DREN networks to the SDP-L

e) provide the Subscriber with IP address and port/protocol information for the tunnel endpoints (e.g., to configure a Subscriber managed firewall exception)

f) provide the Subscriber with DREN IP service provisioning information

SDP-L shall accommodate all situations of connection of opportunity configuration (e.g., static or dynamic addressing, client 802.1X, untagged or 802.1q). SDP-L shall also function in environments where its connection is behind any form of NAT [network address translation].

SDP-L nodes shall be remotely configured, monitored, and managed by the NOC. In the event of outages requiring on-site support, the NOC shall rely on Subscriber site staff to assist in fault diagnosis and repair. In the event of SDP-L equipment failure, the Contractor shall next day ship a replacement SDP-L to be installed by the Subscriber staff and shall include a return shipping label. The Subscriber is responsible for packaging and delivering the failed unit to the shipper. The Subscriber will be responsible for making all physical network connections, applying power, and for ensuring that local infrastructure allows the encrypted tunnel traffic to pass. If a Subscriber network situation change impacts the tunnel, the Subscriber will notify the NOC, and the NOC shall update the SDP-L and TTP configurations as appropriate.

At the location where the SDP-L is installed, the Subscriber will be responsible to meet all DoD security requirements. The Subscriber will describe the exact location of SDP-L equipment to the Contractor, and notify the Contractor if the equipment is relocated.

All management shall be performed in-band (inside the secure tunnel).

SDP-L shall support standard DREN services, with the exceptions in Table 6.9 SDP-S requirements changed to "best effort" in SDP-L and Table 6.10 SDP-S requirements removed or replaced in SDP-L.

SDP-L shall include at least four 1G copper interfaces, one for the uplink to the connection of opportunity and three for Subscriber connections.

SDP-L shall connect to DREN via multiple encrypted (e.g., IPsec) tunnels to Government specified TTPs. Two such TTPs (primary and backup, regionally separate) shall be utilized for redundancy. The encrypted tunnels shall utilize technology that will operate over a standard commodity IP (IPv6 preferred) network. The Ethernet

Service shall be provisioned via the encrypted tunnels. Although the Government desires 1500 byte MTU Ethernet service, the Contractor shall support at a minimum 1300 byte Ethernet frames.

Subscribers will connect to the SDP-L in the same way as to a standard SDP, via Ethernet VLANs. SDP-L itself is just a layer-2 (Ethernet) service, and does not include any routing capabilities, as all the IP service is at the DCN or other DREN Nodes with a Router Function.

Upgrading from SDP-L to an SDP-S is not a requirement.

Table 6.9 SDP-S requirements changed to "best effort" in SDP-L

Performance (6.1.0.2)
Buffering (6.1.0.3)
Ethernet QoS (6.1.1.3)
Frame Size (6.1.1.6) support for 9154 byte frames
IP MTU (6.1.2.3) support for 9000 byte packets
Transport Performance (6.1.3)
IP QoS (6.1.2.7)
Documentation (6.5.13, and elsewhere throughout PWS)
Acceptance Testing (6.5.14)

Table 6.10 SDP-S requirements removed or replaced in SDP-L

Ethernet Multicast (6.1.1.2)
MACsec Encryption (6.1.1.5)
MACsec requirement included in Resiliency (6.1.1.7)
Multicast (6.1.2.5)
DREN Node Line Rate (6.2.0.3) greater than 1 Gbps
Traffic Mirroring, VLAN translation, and Provider Backbone Bridging in Switch Function (6.2.1)
Ports (6.2.1.1) and Modules (6.2.1.2) other than 1G Copper
Optional Functions, including Switch (6.2.1.4), Router (6.2.2), Firewall (6.2.3), Compute (6.2.4)
Intrusion Detection Systems (IDSs) (6.3.6)
Service Provisioning (6.5.1)
Any on-site support (e.g., 6.4.2 6.5.6)
Out of Band Access (6.5.11)

6.2.10. Tunnel Termination Point (TTP) (Separately Orderable)

The Contractor shall provide a tunnel termination service in support of the SDP-L nodes that use encrypted tunnels over the Internet to establish connectivity to DREN. This service is implemented at specific DCNs, and each instance of this service is a TTP. The TTP shall encrypt and decrypt tunnels and extend the contained VLANs to their associated broadcast domains (VLAN/Bridge) in the DCN switch function. The TTP shall be fully compatible with and be able to support any of the SDP-L node capabilities. SDP-L nodes shall connect to

multiple TTPs for resiliency, and the tunnel termination service shall support failover from its designated primary TTP to its backup TTP during any outages along the path to the primary TTP, and shall revert from backup to primary when the path to the primary TTP is restored. Each TTP shall support an aggregate of 10 Gbps of tunnel traffic.

6.3. Security

The Contractor shall perform all necessary actions to ensure all applicable security requirements (e.g., DoD, National) are met which includes cyber, physical and personnel security.

Cybersecurity is defined as the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

The Contractor shall comply with all security regulations, instructions, publications, orders, and policies (as revised, updated, amended, changed or superseded) including:

a) DoD Instruction (DoDI) 8500.01, "Cybersecurity," March 14, 2014

b) DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

c) NIST Special Publication (SP) 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010, as amended

d) NIST SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," current edition.

e) Committee on National Security Systems Instruction (CNSSI) 1253, "Security Categorization and Control Selection for National Security Systems," March 15, 2012, as amended

f) NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," current edition

g) NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans," June 2010, as amended

h) Section 11331 of Title 40, United States Code

i) Committee on National Security Systems Policy (CNSSP) 22, "Policy on Information Assurance Risk Management for National Security Systems," January 2012, as amended

j) Subchapter III of chapter 35 of Title 44, United States Code (also known as the "Federal Information Security Management Act (FISMA) of 2002")

k) DoDI 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense," July 16, 2008, as amended

l) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)" Current as of 9 June 2015.

m) CJCSM 6510.02, "Information Assurance Vulnerability Management (IAVM) Program," November 5, 2013.

n) DoD Directive 8140.01 "Cyberspace Workforce Management," Incorporating Change 1, July 31, 2017

o) DoD 8570.01-M, "Information Assurance Workforce Improvement Program," Incorporating Change 4, 11/10/2015

p) Strategic Instruction (SI) 527-01 27, March 2015, “Department of Defense (DoD) Information Operations Condition (INFOCON) System Procedures”.

Commensurate with supporting the High Performance Computing Modernization Program (HPCMP) mission, and the value of potentially affected information or assets, the HPCMP has implemented a cybersecurity risk management process as prescribed by DoDI 8500.01. The process is used to manage risk and to leverage the process as described in NIST SP 800-39 and CNSSP 22.

The purpose of the Defense Cybersecurity Program is to ensure that Information Technology (IT) can be used in a way that allows mission owners and operators to have confidence in the confidentiality, integrity, and availability of IT and DoD information.

Managing Cybersecurity risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders planning and managing DoD operations, to individuals developing, implementing, and operating the IT that supports those operations. Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions, as defined in DoDI 5200.39, which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other acquisitions of DoD.

The HPMCP has employed a comprehensive IT security governance structure that provides assurance that IT security strategies are aligned with the HPCMP's mission and business objectives; is consistent with applicable laws and regulations through adherence to policies and internal controls; and provide assignment of responsibility. The HPCMP Cybersecurity Program provides the mechanisms to measure, monitor, and enforce information security and sharing policies and procedures as they relate to information in an electronic form, primarily through the implementation of security controls.

Cybersecurity shall be fully integrated into system life cycles and will be a visible element of HPCMP, External Services, joint, and DoD Component IT portfolios. All IT that receives, processes, stores, displays, or transmits DoD information will be acquired, configured, operated, maintained, and disposed of consistent with applicable DoD and HPMCP cybersecurity policies, standards, and architectures.

All IT identified as supporting the HPMCP is under the governance of the HPCMP Cybersecurity Program in accordance with DoDI 8500.01. The cybersecurity requirements for DoD information technologies is managed through the RMF DoDI 8510.01 and is consistent with the principals established in NIST SP 800-37.

The RMF satisfies the requirements of Subchapter III of Chapter 35 of Title 44, United States Code (U.S.C.), also known and referred as the "Federal Information Security Management Act (FISMA) of 2002". IT supporting the HPCMP shall meet or exceed the standards required by the Office of Management and Budget (OMB) and the Secretary of Commerce, pursuant to FISMA and Section 11331 of Title 40, U.S.C.

DoDI 8510.01 describes the DoD RMF process for identifying, implementing, assessing, and managing cybersecurity capabilities and services, expressed as security controls, and authorizing the operation of IT and Platform IT (PIT) systems. Contractor personnel serving in RMF roles at every level shall refer to NIST SP 800-37 for a full description of the process, definitions, roles and responsibilities, and activities. In cases where NIST SP 800-37 conflicts with DoDI 8510.01, compliance with DoDI 8510.01 takes precedence and shall be required.

In the categorization process, the Information Owner (IO) identifies the potential impact (low, moderate, or high) resulting from the loss of confidentiality, integrity, and availability if a security breach occurs. The HPCMP Authorizing Official (AO) has categorized DREN as having a Confidentiality value of Moderate, an Integrity value of Moderate, and an Availability value of Low (overall C.I.A. value of MML), in accordance with CNSSI 1253. Therefore, the Contractor shall implement a corresponding set of security controls from NIST SP 800-53, and use the assessment procedures from NIST SP 800-53A.

The HPCMP has an established AO who is responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture. All IT under HPCMP authority will comply with the RMF and operate only authorized IT and PIT systems (i.e., those systems under a current Authorization to Operate (ATO) or Interim Authorization to Test (IATT)).

6.3.1. RMF Support

The Contractor shall:

a) support the Government's accreditation of DREN in accordance with DoDI 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT)” and any supplemental guidance or instructions for DoD Information Technology

b) designate at least two qualified IAM Level I individuals as Information System Security Officers (ISSOs) within 10 days after contract award to coordinate with the Government (including the DREN Information System Security Manager (ISSM)), System Owners, Contractor System and Network Administrators, and other stakeholders

c) ensure that all ISSOs (non-ISSOs may also):

   1) complete DISA Enterprise Mission Assurance Support Service (eMASS) training

   2) meet all other requirements to establish eMASS accounts within 30 days after contract award

   3) maintain eMASS accounts throughout the life of the contract

d) gather and upload DREN accreditation artifacts to the DREN eMASS RMF System Record Artifact section; perform document composition; map all security controls to an associated artifact and upload DREN eMASS self-assessment results

e) deliver, via the Government Documentation Repository, all draft required RMF documents (e.g., Standard Operating Procedures (SOPs), Concept of Operations (CONOPS), System configurations and RMF Plan documentation) to meet security controls in editable Microsoft Office Word format

f) deliver, via the Government Documentation Repository and uploaded into eMASS, all final version required RMF documents (e.g., SOPs, CONOPS, System configurations and RMF Plan documentation) to meet security controls in Adobe PDF format that shall be digitally signed by the Contractor's Program Manager (PM) and an ISSO as complete, compliant and accurate

g) deliver, via the Government Documentation Repository, all draft physical, logical, and flow network diagrams in Microsoft Office Visio format and PDF format, and ensure that each diagram includes a legend that identifies the creator, version number, original and modification date, validation date, geographic location, and type of diagram, e.g., physical or logical. Each diagram shall also identify the building(s) and room number(s) in which the equipment is located. Industry standard graphics shall be used for consistency of all the diagrams. Physical network connections such as Copper (CAT5E [Category 5 enhanced]/CAT6A [Category 6 augmented]) or fiber (MM/SM) shall be identified. All rooms shall be identified in which any network connection terminates or interconnects

h) deliver, via the Government Documentation Repository, all final versions of physical, logical, and flow network diagrams in Microsoft Office Visio format and Adobe PDF format. Final Adobe PDF versions of physical, logical and flow network diagrams shall be digitally signed by the Contractor's PM and an ISSO as complete, compliant and accurate. These signed PDFs shall be uploaded into eMASS as DREN RMF Artifacts. Within 15 days of any change to the physical, logical, or flow aspects of the network the Contractor shall upload updated artifacts

i) deploy the following Government provided security monitoring and vulnerability assessment tools prior to the commencement of the DREN IPC Demonstration to begin continuous monitoring; controlling and validating the security posture of all DREN deployed networking and support hardware and components; as well as providing artifacts required for the DREN RMF package

    1) Assured Compliance Assessment Solution (ACAS)

    2) Security Content Automation Protocol (SCAP) Tools

    3) Security Technical Implementation Guide (STIG) Viewer

    4) Rapid AuDit of unIX (RADIX) Agents

    5) Host Based Security System (HBSS) Agents

    6) DJS

j) establish sufficient network paths between the Contractor's DREN network support and network management enclaves and the other DREN networks to permit traffic to the Cybersecurity Services Provider's (CSSP) enclave 90 days after Government acceptance of the DREN IPC demonstration to support data feeds from monitoring and vulnerability assessment tools

k) provide all networking and support system IP addresses and hostnames to the Government to enable the Government to validate that the deployed monitoring and vulnerability assessment tools are properly evaluating all Contractor DREN networking and support systems

l) maintain and update the DREN RMF package throughout the life of the contract

m) ensure that the DREN RMF package continually reflects the physical, logical and address/hostname configuration and security status of DREN and its supporting components

n) configure IT products as defined in DoDI 8500.01 in accordance with the latest applicable DoD STIGs and DoD Security Requirements Guides (SRGs)

o) instantiate the RMF self-assessment process by first evaluating the STIG compliance, producing STIG checklist(s) and then import these into eMASS. Continue to evaluate all remaining RMF security controls. All results shall be recorded in eMASS using the following marking methodology

   1) if a security control vulnerability is not found (observable, technical, or lack of documentation), the security control is recorded as Compliant with evidence provided in the test result

   2) if a security control vulnerability is found, the security control is recorded as Non-Compliant, and a Plan of Actions and Milestones (POA&M) line item shall be initiated. The POA&M is required for any assessment decision that requires corrective action or risk acceptance by the HPCMP AO. Weaknesses identified on the POA&M reflects residual risk to the system. Each POA&M line item shall include a mitigation statement, procedures and actions to be taken if any, and milestone dates by which the security control vulnerabilities will be remediated or a statement to justify the HPCMP AO accepting the existing residual risk

   3) security controls that are not technically or procedurally relevant will be recorded as Not Applicable (NA) and a POA&M line item will be initiated with a valid explanation as to why the control is NA

p) meet all POA&M milestone dates. All milestone dates and any changes to them shall be approved by the Government

To support the completion of the DREN RMF package, the Government will provide the following to the Contractor upon contract award:

a) C.I.A. Impact Memorandum to set requirements for the security control baseline.

b) DREN RMF Artifacts that require tailoring to reflect the DREN deployment

c) eMASS training link

d) The following RMF Artifact Templates:

   1) Audit and Accountability Plan

   2) Configuration Management Plan

   3) Contingency Plan

   4) Access Control Plan

   5) Incident Response Plan

   6) Information Systems Maintenance Plan

   7) Physical and Environmental Protection Plan

   8) System and Communication Protection Plan

9) System and Information Integrity Plan

The Government will perform the following to support the completion of the DREN RMF package:

a) Approve and generate Contractor eMASS accounts when all eMASS account requirements are met by personnel designated by the Contractor.

b) Create the eMASS record for the DREN accreditation.

c) Evaluate test results for each applicable RMF security control.

d) Review Contractor created POA&M for non-compliant controls.

e) Review and evaluate CSSP Alignment Artifacts

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.3.1	RMF Artifacts	Contractor-Determined Format	Within 15 days after any change to the physical, logical, or flow aspects of the network or other security impacting changes		eMASS filings; RADIX uploads; ACAS filings; and other CSSP uploading and filing requirements	Every time there are significant changes

6.3.1.1. RMF IATT Package

In order to proceed with the migration of DREN III to DREN4, the minimum RMF requirements as specified in this subtask shall be completed and the overall residual risk of the systems that will be utilized to support the movement of DoD traffic shall be at an acceptable level as determined by the HPCMP AO.

Therefore, to achieve an IATT the Contractor shall (per the schedule in 6.6 Implementation and Transition):

a) tailor the template and deliver the Final Draft RMF documents to comply with security control requirements necessary for the issuance of an IATT including:

1) Final Draft Configuration Management Plan

2) Final Draft Contingency Plan

3) Final Draft Incident Response Plan

4) Final Draft Network Management Plan

5) Final Draft Maintenance Plan

6) Final Draft Physical and Environmental Protection Plan

b) develop and/or deliver the following initial DREN4 RMF artifacts to comply with security control requirements necessary for the issuance of an IATT:

1) Applicable STIG/SRG manual and benchmark reports for all DREN4 deployed hardware

2) Final Draft Physical and Logical Network Diagrams

3) Hardware and Software Lists for all DREN4 deployed networking and support hardware and components

4) Baseline network device, ACLs, ports/protocols/services list, firewall and host configurations for all DREN4 deployed hardware

5) Final Draft CONOPS

6) Final Draft Systems Security Plan (6.3.1.2.1 Systems Security Plan)

c) perform and complete self-assessments and submit in eMASS mapping each control to an artifact(s) in eMASS

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.3.1.1	RMF IATT Artifacts	Government provided templates to be provided after award	220 days after contract award		eMASS filings; RADIX uploads; ACAS filings; and other CSSP uploading and filing requirements	One Time

6.3.1.2. RMF ATO Package

The Contractor shall complete the requirements as specified in this subtask such that the overall residual risk of the systems that will be utilized to support the movement of DoD traffic are at an acceptable level as determined by the HPCMP AO before the HPCMP AO will grant a DREN ATO.

Therefore, to achieve an ATO the Contractor shall deliver the following RMF artifacts in accordance with the schedule in (6.6 Implementation and Transition):

a) Final CONOPS

b) Final Configuration Management Plan

c) Final Contingency Plan

d) Final Incident Response Plan

e) Final Network Management Plan

f) Final Maintenance Plan

g) Final Physical and Environmental Protection Plan

h) Final Systems Security Plan (6.3.1.2.1 Systems Security Plan)

i) Final Physical and Logical Network Diagrams

j) Access Control Plan

k) Audit and Accountability Plan

l) Services and Acquisition Plan

m) System and Communication Protection Plan

n) System and Information Integrity Plan

o) Completed SCAP scans for all deployed systems in Continuous Monitoring and Risk Scoring (CMRS) format

p) Completed ACAS scans for all deployed systems

q) Complete RADIX assessment and uploads for all deployed systems

r) Completed POA&M

s) Baseline configuration images for all deployed network devices, support and peripheral systems

t) Applicable STIG/SRG manual and benchmark reports for all DREN deployed hardware

u) Completed eMASS self-assessment of the DREN RMF package

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.3.1.1	RMF ATO Artifacts	Government provided templates to be provided after award	243 days after contract award		eMASS filings; RADIX uploads; ACAS filings; and other CSSP uploading and filing requirements	One Time

6.3.1.2.1. Systems Security Plan

The Contractor shall develop a System Security Plan in accordance with NIST 800-53 that:

a) Is consistent with the HPCMP enterprise architecture

b) Explicitly defines the authorization boundary for DREN

c) Describes the operational context of DREN in terms of missions and business processes;

d) Include the security categorization of DREN including supporting rationale.

e) Describes the operational environment for DREN and relationships with or connections to other information systems and or networks

f) Provides an overview of the security requirements for DREN

g) Addresses all security controls required for the Information System Security Categorization C.I.A. level of MML

h) Identifies any relevant overlays, if applicable

i) Describes the security controls in place, or planned, for meeting those requirements including a rationale for the tailoring decisions

j) Is reviewed and approved by the HPCMP AO prior to plan implementation

In addition, the Contractor shall:

a) Review and update the System Security Plan within 14 days of any change to any function, capability, component or service provided; or to address problems identified during the plan implementation or security control assessments; or annually when no changes have occurred.

b) Protect the System Security Plan from unauthorized disclosure and modification.

6.3.1.3. Continuous Monitoring

Information Security Continuous Monitoring (ISCM) is very complex and requires a close working relationship between the Government and the Contractor. The Contractor shall ensure the overall risk to DREN is minimal and remains acceptable to the HPCMP AO. The Contractor shall perform ISCM of DREN to monitor security risk and increase situational risk awareness in accordance with the following ISCM instructions: DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)"; NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations; and OMB Circular A-130, Managing Information as a Strategic Resource. This requirement includes that the Contractor shall:

a) perform reviews of Government specified DREN RMF package security controls according to ISCM instructions and provide evidence via a monthly report, no later than the 15th of each succeeding month, that the required review has been performed

b) acknowledge, review, respond to, and act upon:

1) the output of automated and manual cybersecurity vulnerability scanning/assessment tools

2) all IAVM notifications

3) cybersecurity Service Provider (CSSP) alerts and assessment and vulnerability reports

4) anomalies detected in log files

5) generated Cybersecurity related alerts

6) other assessment and vulnerability reports

c) ensure that non-IAVM findings are remediated by the required times in Table 6.11 Non-IAVM Findings required remediation times. If a finding cannot be remediated by its suspense date due to a technical or logistical reason, a POA&M line item shall be created and the reason for the POA&M line item shall be reported in the Monthly POA&M Status Report

Table 6.11 Non-IAVM Findings required remediation times

High and critical risk findings	Shall be remediated prior to receiving an ATO
High and critical risk findings identified through continuous monitoring activities	Shall be remediated within 30 days after identification.
Moderate findings	Shall be remediated within 90 days following identification.
Low findings	Shall be remediated within 180 days following identification.

d) ensure that applicable IAVAs [Information Assurance Vulnerability Alerts] and IAVBs [Information Assurance Vulnerability Bulletins] are mitigated by the required suspense date. If remediation by the suspense date is not possible due to a technical or logistical reason, a POA&M line item shall be created and the reason for the POA&M line item shall be reported in the Monthly IAVM Status Report due by the 15th of each month.

e) deliver a monthly IAVM Status Report in Microsoft Office Excel format no later than the 15th of each succeeding month that includes the following for each IAVM: IAVM Notice, Description, Acknowledge Suspense Date, Acknowledge Date, Applicable (yes/no), Action Suspense Date, Estimated Completion Date, POA&M Required (yes/no), POA&M Created, POA&M Suspense Date, and POA&M Completion Date

f) conduct at least once in each contract year, Federal Information Security Management Act (FISMA) reviews of the Government designated (provided at issuance of the ATO and updated later by the Government) DREN RMF security controls for compliance via eMASS

g) maintain POA&Ms in eMASS on a continuous basis. All POA&M entries shall map back to a finding. Each finding in the POA&M shall have a unique identifier from the issuing authority that pairs with the finding

h) review all residual risks on a monthly basis and if applicable update the DREN RMF POA&Ms in eMASS

i) review all POA&M milestones on a monthly basis and identify any issues and time variances to the ISSM. If changes are approved update the POA&M in eMASS

j) revalidate all physical, logical, and flow network diagrams every 180 days. Update the network diagrams including at minimum updating the legend validation date. Upload to the Government Documentation Repository (draft and final) and to eMASS (final). The update and upload shall be accomplished within 15 days of the revalidation

k) resubmit DREN RMF artifacts via eMASS that require update within 15 days after any of the following

    1) observation of undocumented change to physical, logical, or flow configuration

    2) observation of any undocumented changes to procedures, vulnerabilities, or any other artifacts

    3) after each Security Control Assessor-Validator (SCA-V) Assess and Authorize Security Assessment

l) within 15 days of any hardware or software change, perform and complete self-assessments and submit in eMASS

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.3.1.3	Control Review Report	Contractor determined format	243 days after contract award		eMASS filings; RADIX uploads; ACAS filings; and other CSSP uploading and filing requirements	One Time
	POA&M Status Report	Contractor determined format	15th of each month		Standard Distribution (6.0.2) plus the DREN ISSM	Monthly
	Physical, Logical, and Flow Network Diagrams	Contractor determined format	Within 15 days of every 180 day revalidation		Upload to the Government Documentation Repository (draft and final) and to eMASS (final)	Every 180 days
	Resubmitted RMF Artifacts	Contractor-Determined Format	Within 15 days after any change to the physical, logical, or flow aspects of the network or other security impacting changes, and every SCA-V assessment		eMASS filings; RADIX uploads; ACAS filings; and other CSSP uploading and filing requirements	Every time there are significant changes or a SCA-V assessment

6.3.2. Configuration Control Board Change Requests

Any substantive and/or architectural change to DREN, including system hardware, system software, functionality, and capability, requires approval of the DREN Configuration Control Board (CCB). Therefore, the Contractor shall:

a) Develop the CCB Change Request in accordance with the latest version of the DREN CCB Charter

b) Establish a Contractor Engineering Review Board (ERB) which shall review, adjust and approve all Requests

c) Submit (per the DREN CCB Charter) all ERB approved CCB Change Requests including evidence of that approval

d) Implement the change documented in the Request (as updated) only after receiving the DREN CCB Chair approval.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.3.1.3	CCB Change Request	Contractor determined format	30 days prior to requested change date		Standard Distribution (6.0.2)	As required

6.3.3. Network Protections

In the event of a cyber-attack which affects DREN, the Contractor shall apply both automatic and manual protections (e.g., block, rate limit) to mitigate the loss of resources. Examples of such cyber-attacks include Denial of Service (DoS), DDos, and other types of amplification attacks. These protections shall be placed as close to the source of the attack as possible, such as inside of DREN or within an external (upstream) peer.

When protections are applied (whether automatically or manually), notifications shall be sent to the Government per 6.5.5.1 Notifications.

6.3.4. Initial Boundary Protection Deployment

The Contractor shall implement ingress and egress layer 2, layer 3, and layer 4 filters, ACLs, and firewall policies. The Government will provide these using a Government defined format. The Contractor shall translate from this format and apply these controls to any Switch, Router and Firewall Function(s) as directed by the Government.

6.3.5. INFOCON/CPCON Changes

The Government is required to take necessary actions in response to changes in INFOCON/Cyber Protection Condition (CPCON) levels in order to protect DREN and the DoD Information Networks (DoDIN) against adversarial attacks. Changes to the levels will be tasked by Joint Force Headquarters-DoD Information Networks (JFHQ-DODIN).

To support INFOCON/CPCON DREN tasking, the Contractor shall implement network boundary configuration changes including ACLs, firewall filters, and any other security changes at the Security Change Priority as specified in (6.5.2 Change Request Provisioning)

6.3.6. Intrusion Detection Systems (IDSs)

The Contractor shall:

a) support the deployment of Government IDSs in the form of function (6.2.7 Rack Space (separately orderable), 6.2.4.3 DJS Compute Function, and 6.2.1 Switch Function (One included)g) mirror traffic) and/or touch labor (6.5.16 Touch Labor) at DREN locations specified by the Government

b) not enable traffic exchange with an external network until the Government has indicated that IDS monitoring is established

c) follow Government policy regarding the exchange of traffic with external networks in the event of a monitoring capability failure

6.3.7. Network Management

The Contractor shall:

a) ensure the protection and separation of infrastructure and network management data from modification while transported through or contained within the Contractor's infrastructure. Network

management data includes accounting, authorization, configuration, fault, performance, and security management data

b) provide the following network management security protection measures

1) authentication of management traffic

2) network management data confidentiality

3) identification and two factor authentication of personnel conducting management operations on each network and support component

4) regulate access by authorization levels

5) component interface/port protection

6) isolation and controls between different management levels and networks in coordination with input from the Government

c) assure that all management traffic is protected from compromise of confidentiality, integrity and availability

d) ensure that all routing neighbor relationships are authenticated in compliance with relevant security controls

e) apply route filtering as directed by the Government

6.3.8. SDREN

The Secret Defense Research and Engineering Network (SDREN) is a government managed Secret network overlay on DREN.

The Contractor shall create local SDREN enclave(s) for communicating classified information in support of U.S. Cyber Command and/or JFHQ DODIN Task Orders, situational awareness, and other security-related tasks as directed by the Government.

The Government provides the Type-1 encryptor, core router, and core switch to deliver SDREN.

These SDREN local enclaves shall be directly accessible by all NOC staff with responsibilities in security-related tasks (e.g., network administrators, system administrators, and security staff). If there are multiple sites for the NOC staff then multiple independent SDREN locations shall be established. The Contractor shall provide the local enclave hardware (e.g., firewall(s), switch(es), workstation(s)) at the required location(s). The Contractor is responsible for the security authorization process of the local enclave. The Contractor shall complete all actions to plan, coordinate, and establish service from SDREN. The Contractor shall complete the following activities in order to have an operational SDREN Node at the required location(s) no later than 180 days after commencement of Phase II of Transition (6.6.2 Phase II):

a) Establish a closed area certified to process Secret level data in accordance with DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) at the required location(s).

b) Establish a Communication Security (COMSEC) account that can receive secret keying material and cryptographic devices in accordance with DoD 5220.22-M, NISPOM.

c) Acquire Secure Terminal Equipment (STE) telephone system(s) and cryptographic card(s) for use in classified telephone conversations with the Government.

d) Obtain the ATO of the Contractor's systems required to support this task via the Defense Counterintelligence and Security Agency (DCSA) Office of the Designated Approving Authority (ODAA) Business Management System (OBMS).

e) Comply with all SDREN Connection Approval Process requirements and deliver all required SDREN Connection Approval Process (CAP) documentation via the Government Documentation Repository. The Government will provide SDREN CAP upon contract award.

f) Establish access to SDREN email, JIGSAW, ACAS and ePO. At minimum, the Contractor shall submit to the Government completed DD 2875s for personnel requiring accounts.

g) Deploy the following Government provided security monitoring and vulnerability assessment tools to begin continuous monitoring; controlling and validating the security posture of all deployed networking and support hardware and components; as well as providing artifacts required for the security packages:

    1) ACAS

    2) RADIX Agents

    3) HBSS Agents

    4) SDREN Joint Sensor (SJS)

h) Ensure that access to all Contractor's systems required to support this task is controlled using Classified DoD PKI and/or 2-Factor Authentication.

i) Acquire and utilize a DoD approved middleware and software solution to read Tokens required to support Classified DoD PKI.

j) All staff required to have access to SDREN shall apply through the established Government process for the issuance of Government supplied Classified DoD tokens.

Additionally, the Contractor shall perform the following throughout the life of the contract:

a) Maintain and operate the Secure Terminal Equipment (STE) telephone system(s) and cryptographic card(s).

b) Maintain the ATO (covering the Contractor's systems required for this subtask) via the DCSA OBMS.

c) Maintain the closed area(s) certification, and COMSEC Account.

d) Maintain constant connectivity to SDREN.

e) Review, respond to, and act upon findings in accordance with the requirements of 6.3.1.3 Continuous Monitoring for systems and enclaves on SDREN.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.3.8	SDREN CAP documentation	Government provided format after contract award	No more than 180 days after commencement of Phase II of transition		Standard Distribution (6.0.2)	One time, update as required

6.4. Management

6.4.1. Management Oversight

The Contractor shall perform all necessary actions to ensure all applicable management requirements are met.

6.4.1.1. 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 an organizational approach 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.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.1.1	Program Task Management Report	Contractor-Determined Format (includes presentation, minutes and associated materials)	15th of each month		Standard Distribution (6.0.2)	Monthly

6.4.1.2. 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 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 30 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 fully interoperable with VTC capabilities used by DREN.

6.4.1.3. Project Management Planning and Control

The Contractor shall develop a management schedule for meeting the requirements set forth in this contract within 30 days following contract award. 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.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.1.3	Project Management Planning and Control Report	Contractor Determined Format	30 days after Contract Award and seven days after any substantive changes occur		Standard Distribution (6.0.2)	Any time there is a substantive change

6.4.1.4. Other Direct Cost (ODC) Management

When directed by the Contracting Officer the Contractor shall obtain contract related materials (e.g., supplies, equipment, support) to meet the overall requirement. Those materials must be associated with the overall functions being performed through this contract. The Contractor shall abide by the requirements of the FAR and other DoD Mandatory sources when acquiring supplies and/or materials such as obtaining quotes, documentation of these quotes and submission for approval by the KO. Documentation of purchases will be input into the Government reporting system in order for the Government to review them upon request and to ensure compliance with federal procurement regulations. All supplies shall be authorized by the KO and comply with all applicable requirements.

6.4.1.5. 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 monthly basis. The monthly progress report will identify significant activities, problems, and accomplishments during the preceding month. The monthly report shall also identify significant areas of technology improvement within the Contractor's core infrastructure.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.1.5	Progress Report	Contractor Determined Format (risk management, resources, task completion, significant activities, accomplishments)	4 days after weekly status meeting		Standard Distribution (6.0.2)	Weekly

6.4.1.6. DREN Meetings

The Contractor shall participate upon request in various meetings to include Technical Interchange Meetings (TIMs), Weekly Status Meetings, Technical Advisory Panel (TAP), Hawaii Intranet Consortium (HIC), DREN Engineering and HPC Security.

6.4.1.6.1. Technical Interchange Meeting (TIM)

The Contractor shall provide support to the DREN TIM on an annual basis to inform the DREN community (Government and Federal Contractors) on topics including network performance, status and plans for the coming year. The Contractor shall assist in the development of the agenda, capture minutes, and create presentations regarding various DREN topics such as new technologies, engineering activities, demonstration of networking tools/reports, DREN operations, routing architecture, and network backbone.

TIM meetings will take place at a location determined by the Government.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.1.6.1	TIM Presentations	Government provided prior to TIM	21 days prior to the TIM		Standard Distribution (6.0.2) and presented at the meeting	Annually
	TIM Minutes	Contractor Determined Format	Seven days after the TIM		Standard Distribution (6.0.2)	

6.4.1.6.2. Contract Status Meetings

The Contractor shall participate in bi-weekly Contract Status Meeting with the KO and the Government. The Contract Status Meeting will identify current contract actions completed or pending; outstanding issues; current financial activities including monthly accruals and outage credits; and current/pending network pricing, ordering and implementation activities.

These Contract Status Meetings shall take place via VTC/Telephone or at a location determined by the Government.

6.4.1.6.3. Technical Advisory Panel (TAP)

The DREN TAP is a working group under the government DREN Program Manager (PM). The TAP consists of HPCMP personnel, key organization/site representatives, and significant COI representation. The Contractor shall assist in the development of the agenda and create presentations or discussion frameworks regarding various DREN topics such as new technologies; engineering activities; network modifications, upgrades and improvements; networking tools/reports; DREN operations; routing architecture; and network backbone. The Contractor shall assist in the preservation of discussions by capturing notes during the meeting and providing them to the Government.

These TAP meetings will take place at a location determined by the Government.

6.4.1.7. Asset and Configuration Management

Configuration Management is the process that preserves the integrity of the network configuration. The DREN CCB will control all changes made to the network and related systems provided under this contract. 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 the Government with access to the Contractor's network management database containing configuration management data. This capability shall allow the Government 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) IPv6 and IPv4 subnet structure, routing table configurations

b) multicast configurations

c) network management and external ACLs and/or firewall configurations

d) network device (Core and DREN Node) configurations in general

e) access link identification

f) state of the network elements (e.g., in service, out of service for routine or diagnostic test, disconnected, new)

g) inventory of ports and services at each DREN Node

h) any other equipment installed by the Contractor to provide service such as, network management and monitoring, NOC / help desk information systems, power, rectifiers, UPS [Uninterrupted Power Supply], HVAC, etc.

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

6.4.1.8. Program Management Review (PMR)

The Contractor shall conduct monthly PMRs that address all aspects of the DREN tasks including at minimum:

a) new implementations

b) status of technical and programmatic progress and issues

c) significant infrastructure changes within and outside the DREN network infrastructure

d) outstanding Technical Insertion Proposals (TIPs)

e) CCB Requests

f) DREN peering

g) engineering activities

h) NOC activities

i) site over/under-utilization

j) DNS status/discrepancies

k) security activities

Each review, at a minimum, shall focus on achievements since the last review, the success of risk management activities, resolved and unresolved issues, and action items.

These review meetings shall take place monthly at a location mutually agreed to by the Government and Contractor.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.1.8	PMR Report	Contractor Determined Format (presentations, minutes, and associated materials)	15th of each month		Standard Distribution (6.0.2)	Monthly

6.4.1.9. 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, improve performance, reduce costs which can be realized by the Government, improve end-user services, or enhance administrative and management systems for 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 transport network growth

f) trend analyses and projections

g) security measures and impact

h) advanced planning data and contingency plans

i) interfaces with other networks

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 status of technical and programmatic progress, progress towards achieving DREN goals, significant infrastructure changes within and outside the DREN network infrastructure that can be applied to enhance DREN.

The Contractor shall provide all required materials into the 6.5.10.2 Government Documentation Repository to present its capability to the Government for review and acceptance.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.1.9	Annual Planning and Design Review Report	Contractor Determined Format (presentations, minutes, and associated materials)	Presentations 21 days prior to review meeting, minutes Seven days after meeting		Standard Distribution (6.0.2)	Annually

6.4.2. Network Status Reporting

The Contractor shall provide real-time reporting of DREN network status information, via graphical interface to the Subscribers and to the Government. The reporting utility will provide the ability to generate reports automatically and periodically as directed by the Government. Reports shall cover trouble ticketing and fault management activities, network performance or configuration status, security events or status, and accounting information. At a minimum, the Contractor shall provide the following information pertaining to overall network performance during the progress reporting meetings:

a) Individual DREN Node and DREN Node Service availability for all DREN Nodes and interfaces as defined in the DREN Node 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 – For all trouble tickets that require on-site maintenance, the monthly average of the time from inception of trouble ticket until repair personnel are on site is as follows:

$$\text{Mean Time to Respond} = \frac{\text{Total Time in Hours to Respond On-Site}}{\text{Total Number of On-Site Trouble Tickets}}$$

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 Government satisfaction as follows:

1) All trouble tickets without on-site dispatches

$$\text{Mean Time to Restore} = \frac{\text{Total Outage Time in hours Tickets without On-Site}}{\text{Total Number of Trouble Tickets without On-Site}}$$

2) All trouble tickets with on-site dispatches

$$\text{Mean Time to Restore} = \frac{\text{Total Outage Time in hours Tickets with On-Site}}{\text{Total Number of Trouble Tickets with On-Site}}$$

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.2	Network Status Report	Contractor Determined Format (presentations, minutes, and associated materials)	15th of each month		Standard Distribution (6.0.2)	Monthly

6.4.3. Evolution of Services

The Contractor shall provide state-of-the-art digital data transfer services that are constantly evolving. The Contractor shall perform technology insertion efforts and system upgrades to maintain state-of-the-art services, supporting the need to introduce newly available and evolving technologies while maintaining compatibility with standards and existing services.

6.4.3.1. Technology Insertion Proposal (TIP)

The Contractor shall prepare TIPs both when requested by the Government and when the Contractor wishes to propose an improvement to DREN.

Upon availability of new enhancements that can be substituted for, or added to, services identified in the Contract, the Contractor shall prepare and submit a TIP. The Government will determine which, if any, aspects of the TIP will be considered for contract action with the KO. KO inclusion of a TIP on contract unless specifically stated does not exempt the Contractor from any requirement of this Contract or the DoD (e.g., performance requirements, CCB, RMF).

The TIP shall contain, as a minimum, the following information:

a) A description, in detail, of what is being proposed, pointing out the differences between the existing contract items, services and/or terms, and those proposed

b) A specific analysis of the comparative advantages and disadvantages, the performance impact, the Life-Cycle-Costs, etc., between the existing and proposed changes including how existing services are impacted, any existing site modifications, and increase/decrease in energy use

c) A proposed timeline in which the change would be instituted.

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

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.3.1	TIP	Contractor Determined Format	Seven days after Government request or as needed for Contractor initiated		Standard Distribution (6.0.2)	As required

The following sub-elements give several examples of topics the Government may request TIPs for over the life of the contract. The inclusion of these sub-elements in the PWS, however, does not obligate the Government either to request such proposals or to accept any such proposals that are received.

6.4.3.1.1. Commercial Solutions for Classified (CSfC)

CSfC capabilities support transmission of classified data over available networks. The solution proposed would require technologies from the CSfC Components List to be used, in accordance with NSA's published CSfC Capability Packages. Capability Packages and the CSfC Components List can be found by visiting the CSfC Components List page:

https://www.nsa.gov/resources/everyone/csfc/components-list/

6.4.3.1.2. Enhanced Cybersecurity Service (ECS)

ECS is a Department of Homeland Security program to provide an intrusion prevention capability to help US-based companies protect their computer systems against unauthorized access, exploitation and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers. ECS is discussed further:

https://www.dhs.gov/enhanced-cybersecurity-services

A TIP may be requested to provide DREN ECS as a dedicated service augmenting, rather than replacing a Cybersecurity Service Provider (CSSP).

6.4.3.1.3. Boundary Cloud Access Point(s)

Cloud Access Point(s) provide secure connectivity to the DoD authorized CSP(s). The current version of DoD Cloud Connection Process Guide contains the relevant guidance.

6.4.3.1.4. Time Reference Service

A precise time reference may be requested to provide accurate time to Government-furnished systems (e.g., NTP appliances). The time reference service would be required to be within one microsecond of UTC (USNO). The service would support IRIG-B and/or Global Positioning System (GPS) Antenna time reference options. For each location where Time Reference Service is required, the Government would coordinate with the Contractor to determine which time reference option is the most suitable.

The IRIG-B Service will be required to be compliant with IRIG Standard 200-04. Additional details, such as the signal type and physical connection, will be location-specific and identified at the time of the TIP. The Contractor would coordinate with the Government to deliver, test, troubleshoot, and maintain the IRIG-B Service.

The Government requires assistance in installing a GPS antenna and associated cabling between the antenna and the DCN cage because DCNs are located at Contractor facilities. The Government will provide the GPS antenna, cable, and mounting hardware. The Contractor would install the antenna and cabling.

6.4.3.1.5. Contractor provided localized commodity Internet service

Requirements may arise in the future to obtain commodity commercial Internet service at certain SDP locations. Commodity Internet service examples include cable modem service from the local cable TV service provider, 3G/4G/5G data services from cellular providers, satellite data service, business class service from a local provider, and others. In each case, the Government will specify the location that requires the service along with any bandwidth or other minimum performance requirements. The Government will include information on any known local service providers that could potentially meet the requirement.

6.4.3.1.6. Hybrid SDP

Requirements may arise in the future for a hybrid SDP that is a merger of a standard SDP and SDP-L. This hybrid SDP would have both its standard access link plus a connection-of-opportunity supporting an encrypted tunnel to DREN. This would add the DREN Node sub-type of SDP Hybrid (SDP-H). Use case scenarios for this include backup in case of access link failure, or temporary deactivation or loss of the standard access link. The connection-of-opportunity would utilize the same encrypted tunneling approach as for SDP-L, and would use the TTPs. Routing of traffic over the connection-of-opportunity tunnels would be required to be in a standby state, so that automatic failover will occur if the standard access link goes away for any reason, but would be implemented in a way that prevents Ethernet bridging loops.

6.4.3.2. Upgrades

The Contractor shall offer the Government any upgrades, enhancements, improvements, etc. to DREN Nodes that will enhance Government's use of 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. If at any time during the contract the Contractor needs to upgrade or replace any network component including the underlying infrastructure to meet the requirements of the contract, the Contractor shall do so at no cost to the Government. For upgrades that constitute new technology insertions, the Contractor may submit a TIP (6.4.3.1 Technology Insertion Proposal (TIP)).

6.4.3.3. Technical Refresh and Life Cycle Engineering Support

The Contractor shall provide a coherent approach to sustainment, robustness, and advancement for the life of this contract for all DREN network architecture and services. This may include but not be limited to architectural planning, life cycle engineering, or equipment technical refresh that shall be done at no additional cost to the Government to continue to provide for all the requirements of this PWS.

6.4.4. Simulation and Test Labs (Requirements and Status)

DREN is designed to be a leading edge production environment and as such, simulation and test lab capabilities can affect 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 DREN. As part of the process of implementing new features, systems, or

protocols on DREN, the Contractor shall enable access by the Government for visibility, interaction, and possible control of emulation environments where engineering, simulation, and pre-implementation testing are performed. 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.

6.4.5. 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.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.4.5	Accounting Management Report	Contractor Determined Format	15th of each month		Standard Distribution (6.0.2)	Monthly

6.5. Support

The Contractor shall provide a support capability to the Government and DREN Subscribers including:

a) service provisioning and tracking of DITCO-issued service orders

b) change request provisioning requests from authorized Government staff members

c) reporting, tracking, and resolution of all reported and non-reported DREN problems

d) tracking, implementing, and validating change requests

e) providing a Help Desk/NOC function to support all aspects of DREN services

f) provisioning network configuration, utilization, and performance monitoring tools

g) provision the management network to only use IPv6

6.5.1. Service Provisioning

The Contractor shall, in accordance with the terms of all DITCO-issued service orders issued by the Contracting Officer or other designated authorized representative:

a) process the service orders

b) install, modify, terminate, and restore DREN service

c) upon receipt of termination order, identify equipment and/or cabling that shall be removed and any that shall be abandoned in place, as well as deactivate and remove the DREN Node and any configuration on Contractor systems used to support the terminated node within 30 days

d) be responsible for obtaining, provisioning and maintaining all equipment and software for all service orders

e) provision and track all ordered service including the installation, modification, and termination of DREN Service in a service order

f) support new, modified, and termination service orders as delineated in Table 6.12

Table 6.12 Required Provisioning Intervals for DITCO-issued service orders

Service	Not to exceed
Installation of a new DREN Service Delivery Point (SDP)[1]	90 days
Installation of a new DREN Core Node (DCN)[1]	60 days
Installation of a new DREN eXchange Point (DXP)[1]	60 days
Additional or change to Subscriber Port(s)/Interface(s)	15 days
Service termination and clean-up	30 days
Wide Area Network (WAN) data transfer rate Upgrade if a hardware change is required	90 days
Wide Area Network (WAN) data transfer rate Upgrade if a hardware change is not required	30 days
Wide Area Network (WAN) data transfer rate Downgrade	30 days
SDP Relocation	30 days
Separately orderable function and/or services	45 days

[1]separately orderable functions and/or services ordered at the same time as the DREN Node shall be installed at the same time as the DREN Node.

Deviations from the requirements specified in this subtask shall only be approved the Contracting Officer.

The Contractor shall deliver a Service Request Provisioning Performance Weekly Report via the Standard Distribution by each Thursday at 12:00, Eastern Time. This report measures the quality of each Service Request during the period that includes at a minimum the information required in each service ticket (6.5.3.2 Tickets (Service)). The report shall be in a Contractor defined format and contain ticket data, metrics of performance, and explanations when requirements are not met.

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)	
6.5.1 Service Provisioning	Service Provisioning Elements a) through f)	The Contractor delivers service as required from a Government issued Telecommunications Service Order (TSO) and within the timelines specified in Table 6.12 Required Provisioning Intervals for DITCO-issued service orders.	Government review of Service Request Provisioning Performance Weekly Report and individual 6.5.14.2 Acceptance Test Reports.	New Node or upgrade timeline	NRC Plus/Minus
				On time	No +/-
				1-10 days late	-2%
				11-20 days late	-4%
				21-30 days late	-8%
				> 31 days late	-16%

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.1	Service Request Provisioning Performance weekly report	Contractor-Determined Format	Weekly by each Thursday at 12:00, Eastern Time		Standard Distribution (6.0.2)	Weekly

6.5.2. Change Request Provisioning

The Government will issue to the Contractor three types of "Change Requests": "Routine", "Priority", and "Security". Routine change requests may include, but are not limited to, route modification; new or modified VLAN configuration; Subscriber interface configuration modification; and new, modified, or updated DNS entries managed by the Contractor. Priority Change Requests include the same items as Routine Change Requests but are deemed higher priority or need quicker delivery. Security Change Requests are in support of the protection of DREN and its Subscribers and typically would involve ACL or firewall filter modifications. Change requests submitted by Subscribers will always be Routine unless otherwise directed by the Government. The Government will indicate the Change Type when it submits a Change request. The Government may authorize additional Security staff the authority to designate Change Requests as Security Priority.

The time to perform the change starts when the Change Request is delivered to the Contractor.

The time the change is completed is only when proper operation of the Change Request is validated by the requestor.

The Contractor shall:

a) Provision change requests in accordance with Table 6.13 when received from an authorized Government staff member via the 6.5.3 Service Management System (SMS) and/or via a digitally signed e-mail 24x7x365.

Table 6.13 Change Request Required Delivery Intervals

Change Type	Standard
Routine Change Request	12 hours
Priority Change Request	2 hours
Security Change Request	30 minutes

b) Document in monthly reports measurements of the quality of Change Request Provisioning Performance. Delivery of the monthly Change Request Provisioning Performance Report is via the Standard Distribution and shall be no later than the 15th of each month. This report shall include at a minimum:

1) Total Number of Routine Change Request Tickets

2) Percentage of Routine Change Requests completed within the threshold specified in Table 6.13 Change Request Required Delivery Intervals

3) Number of Routine Change Requests not completed within the threshold specified in Table 6.13 Change Request Required Delivery Intervals

4) For each Routine Change Request not completed problem within the threshold specified in Table 6.13 Change Request Required Delivery Intervals provide:

   A) Routine Change Request Ticket number

   B) DREN Node location(s)

   C) Total time to complete the Routine Change Request

   D) Brief description of the Routine Change Request

   E) The reason the Routine Change Request was not completed in the required timeframe

5) Total Number of Priority Change Request Tickets

6) Percentage of Priority Change Requests completed within the threshold specified in Table 6.13 Change Request Required Delivery Intervals

7) Number of Priority Change Requests not completed within the threshold specified in Table 6.13 Change Request Required Delivery Intervals

8) For each Priority Change Request not completed problem within the threshold specified in Table 6.13 Change Request Required Delivery Intervals provide:

   A) Priority Change Request Ticket number

   B) DREN Node location(s)

   C) Total time to complete the Priority Change Request

   D) Brief description of the Priority Change Request

   E) The reason the Priority Change Request was not completed in the required timeframe

9) Total Number of Security Change Request Tickets

10) Percentage of Security Change Requests completed within the threshold specified in Table 6.13 Change Request Required Delivery Intervals

11) Number of Security Change Requests not completed within the threshold specified in Table 6.13 Change Request Required Delivery Intervals

12) For each Security Change Request not completed problem within the threshold specified in Table 6.13 Change Request Required Delivery Intervals provide:

   A) Security Change Request Ticket number

   B) DREN Node location(s)

   C) Total time to complete the Security Change Request

D) Brief description of the Security Change Request

E) The reason the Security Change Request was not completed in the required timeframe

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.5.2 Change Request Provisioning	Change Request Provisioning	The Contractor provisions change requests on time and 100% accurate/error free.	Government validation of change requests and review of Change Request Provisioning Performance Report.	-1% of NOC Monthly Recurring Charge (MRC) per incident of not meeting 100% accurate and on time.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.2	Change Request Provisioning Performance Report	Contractor-Determined Format	15th of each month		Standard Distribution (6.0.2)	Monthly

6.5.3. Service Management System (SMS)

The Contractor shall:

a) Implement a Service Management System (SMS), often implemented in part by a trouble ticket management system, for record keeping and management of problems and their resolution, as well as for tracking security related issues, change requests, DITCO-issued service order, and all maintenance activity before 6.6.1.1.5 IPC Test and Demonstration begins. The SMS shall have the capability to present and sort, at a minimum, the ticket number, ticket type (security, trouble, change request, maintenance, service etc.), ticket priority (Security, Problem/Trouble, Routine/Priority Change Requests, Routine/Emergency Maintenance and Service), ticket status, creation date, DREN Node and Subscriber Enclave(s). Table 6.14 Ticket Types provides ticket priorities, type, and examples.

Table 6.14 Ticket Types

Type	Priority*	Examples for Determining a Ticket Type
Security	1	Any security-related issue such as, but not limited to: a compromise to any Contractor device used to support DREN; DoS or DDoS attack against DREN or devices used to support DREN; IAVM compliance and mitigations; and, DREN Cyber IP or port and protocol blocks.
Trouble	2	Investigating, isolating, and repairing problems related to loss or degradation of: connectivity to management systems, Subscribers, and peering networks, or function of a support system or application.
Change	3	Requests to make network configuration changes, e.g., VLAN addition, Subscriber route changes or additions, whitelist updates, Port and Protocol or Tunnel Exception Requests, as well as changes related to approved CCB requests or approved TIPs.
Maintenance	4	Provider or Subscriber maintenance affecting network or DREN Node operation, Subscriber connectivity, access link provider(s) maintenance, or upgrades to networking or support systems.
Service	5	Support to establish DREN service at a new location, upgrade DREN service at present location, or expand Subscriber port allocation at a present DREN location.

* Priorities indicated do not relinquish the Contractor from any performance requirement specified in this PWS

b) Ensure that all SMS data fields are searchable.

c) Ensure that all SMS data is available to the Government and DREN Subscriber POCs via a secure web-based GUI on a real-time, automated basis.

d) Ensure that user access and authorization to the SMS is controlled by DoD PKI.

e) Ensure that all data exchanges with any component of the SMS are encrypted.

f) Ensure that SMS data is maintained throughout the life of the contract.

g) Develop, implement and utilize a methodology for grouping tickets under a parent - child tracker when multiple tickets are opened on a related issue.

h) Open a ticket in the SMS prior to performing tasking and maintain that ticket until completion or resolution.

6.5.3.1. Tickets (other than "Service" type)

For any ticket of type other than “Service” as indicated in Table 6.14 Ticket Types the Contractor shall:

a) ensure that tickets, at a minimum, provides the following information

1) date and time of ticket opening

2) unique ticket number

3) ticket type and priority

4) name, telephone number and email address of person reporting a security issue, problem, scheduling or reporting a pending maintenance action, or requesting a change

5) if a change request, Name of the Government staff member approving the request

6) name of NOC staff opening the ticket

7) REN Node and Subscriber Enclave

8) data and time of the discovery of a security issue; identification of service loss or degradation; submission of a change request; or the future time of the maintenance event

9) detailed symptom(s), including any developed standard codes for problem classification (agreed between Contractor and Government)

10) detailed description of the security issue, trouble, change, or maintenance action

11) detailed updates to actions taken on all tickets to include date and time each action was taken

12) detailed description of each escalation trigger and action taken, including as required in 6.5.9 Problem Escalation

13) detailed description of all actions taken to resolve a security issue, correct a trouble, implement a change request or complete a maintenance action

14) description of how affected service will be verified as working

15) report of verification of affected service as working

16) date and time of security issue resolution, service restoration, completion of a change request, or end of a maintenance action

17) date and time of closure of the ticket

6.5.3.2. Tickets (Service)

For any ticket with a type of "Service" as indicated in Table 6.14 Ticket Types the Contractor shall:

a) enter all DITCO-issued service orders in its SMS to track and maintain the progress of each service order from origination to completion

b) ensure each service ticket, at a minimum, provides the following information

1) service order type (new, change, move, disconnect, upgrade, or downgrade)

2) service description

3) CSA/PIID number

4) Telecommunications Service Request (TSR) number

5) date of receipt of CSA/TSO from DITCO

6) DREN Node location (actual physical address of delivery location)

7) NPA/NXX [Area Code and Prefix] of the location

8) DREN Node number as designated by the Government

9) DREN Node name as designated by the Government

10) DREN Node Line Rate, ports and interfaces
11) Plain Old Telephone Service (POTS) line Information for new service requests
12) account code
13) calculated required due date
14) primary and alternate DREN Subscriber contact name, address, email, cell number (if provided) and telephone number from the TSR
15) service status (updated at least weekly)
16) FOC [Firm Order Commitment]/access link status (updated at least weekly).
17) site survey schedule date
18) site survey completion date
19) DREN Node installation schedule date
20) DREN Node installation date
21) DREN Node plan and as-built diagram delivery due date
22) acceptance test date and time
23) date service is accepted and ticket is closed

6.5.4. Contractor Managed Network Database

The Contractor shall implement a database that stores DREN configurations and other related information. The database shall contain DREN Subscriber Information, DREN Node Information, DREN Core IP Address Allocations, and VLAN Allocation details.

The Contractor shall:

a) include DREN Node Physical Addresses, Subscriber Port/Interface Information in the database
b) include an IP Address Management Tool to be utilized by the Contractor and Government to manage DREN IP assignments in the database
c) include a VLAN Management Tool to be utilized by the Contractor and Government to manage DREN VLAN assignments in the database
d) include validation processes that compares database to current network configurations and provide a Validation Report on inconsistencies and corrections on a monthly basis
e) include a query engine to execute cross related queries to the Government Portal
f) archive data for the life of the DREN4 contract
g) maintain and keep all information accurate and current throughout the life of the contract

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.5.4 Contractor Managed Network Database	Contractor Managed Network Database	The Contractor maintains a Network Database that is 100% accurate/error free. All errors detected by the Contractor, by the validation process or reported by the Government are corrected within seven days.	Government review of Validation report and spot checks of Network Database.	-.05% of NOC MRC if greater than 5% errors are identified in the month.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.4	Validation Report	Contractor-Determined Format	15th of each month		Standard Distribution (6.0.2)	Monthly

6.5.5. Network Operations Center (NOC)

The Contractor shall have the responsibility for managing all services under this contract. The Contractor shall serve as the focal point for all Subscribers and the Government to send and receive communications about DREN. The Contractor shall provide all facilities including connectivity to the DREN Network to perform the services on this contract.

The Contractor shall:

a) prior to the IPC Test and Demonstration, establish a "Help Desk" function for Subscribers and the Government to indicate security issues, report problems, request changes, provide notification of maintenance actions, ask questions on any aspect of DREN, and to request status on any of these items

b) prior to the IPC Test and Demonstration, establish and publish a toll-free number to call the Help Desk

c) staff the Help Desk with on-location personnel authorized and capable of accepting, processing, and resolving any security issue, trouble report, or change or maintenance request 24x7x365

d) staff the Help Desk sufficiently to assist multiple DREN Subscribers simultaneously 24x7x365

e) accept and process SMS or digitally signed e-mail submitted security, trouble report, change, or maintenance requests 24x7x365

f) address, resolve, and/or complete all service problems, change requests, security issues, and maintenance involving DREN service

g) install and configure a Government approved chat client that supports eXtensible Messaging and Presence Protocol (XMPP) and Off the Record (OTR) Messaging on all Help Desk workstations and ensure all Help Desk staff

1) register for the DREN chat server (instructions to be provided after award)

2) configure the client for the DREN chat server and enable automatic OTR encryption

3) remain online to the chat server and presence marked as “available” for support interactions with Subscribers and the Government

h) respond to Government and Subscriber initiated communications as delineated in Table 6.15 Required Response Times

Table 6.15 Required Response Times

Communications Type	Response time not to exceed
Initial automated response to an incoming phone call	30 seconds
Incoming phone call by Help Desk human operator	120 seconds
Ticket created via the SMS	30 minutes
Email to the Help Desk	1 hour
VTC call to the Help Desk	30 Seconds
Chat/Instant Message/XMPP conversation to the Help Desk	5 minutes

i) Deliver via the Government Documentation Repository a monthly "Response Metric Report", in a format determined by the Contractor, documenting metrics of Required Response Times no later than the 15th of each month that contains:

1) The type and number of each Communications Type (Table 6.15) responded-to within threshold.

2) The type and number of each Communications Type not responded-to within threshold.

3) The percentage of each Communications Type responded-to within threshold.

4) The percentage of each Communications Type not responded-to within threshold

5) Explanation for each instance where required response times were not met.

j) Develop from the Government provided template and deliver via the Government Documentation Repository "Help Desk" SOPs that adequately address the following issues no later than the IPC Test and Demonstration:

1) Network Management Tool Alarms

2) Ticket Priorities

3) Ticket Response Times

4) Subscriber Tickets

5) Required Information Tickets

6) Trouble Ticket Escalation Procedures

7) Change Request Tickets

8) DNS Procedures

9) Security Incident Tickets

10) Outage Reporting and Outage Update Reporting
11) Routine Maintenance Notifications
12) Rescheduling of Routine Maintenance
13) Updates to Routine Maintenance Notifications
14) Critical or Emergency Maintenance Notifications
15) Updates to Critical Maintenance Notifications
16) Post-Maintenance and Follow-Up
17) Shift Turnover
18) Support Etiquette
19) Telephone Communications
20) Electronic Communications (Email, VTC, Instant Messaging)

Perform an annual review of Help Desk SOPs and provide evidence that an annual review was completed.

Perform updates to of Help Desk SOPs as required between annual reviews and deliver SOP updates via the Government Documentation Repository.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.5	Response Metric Report	Contractor-Determined Format	15th of each month		Standard Distribution (6.0.2)	Monthly
	Help Desk SOP	Contractor-Determined Format	Prior to IPC Demonstration		Standard Distribution (6.0.2)	Full document delivered completely once, changes reviewed with Government after

6.5.5.1. Notifications

It is important to communicate via email with DREN Subscribers and the Government in a consistent manner. The Contractor shall use Government provided notification templates for Notifications including e-mail and text messages.

6.5.5.1.1. Outage Notification Methods, Levels, and Intervals

The Contractor shall notify DREN Operations and all Subscribers whenever any network outage occurs via email. There are six outage levels for DREN. Factors such as the operational criticality, the number of affected sites, global functionality, the ability to maintain manageability, and the ability to monitor, mitigate and communicate threats to the network determine the outage level. Table 6.16 describes the outage levels:

Table 6.16 Outage Level Descriptions

Outage Level:	Description:
Security	A compromise of any kind on any DREN management system or core component and/or a DoS or DDoS attack which affects the functionality of the network itself or the ability to manage the network.
Critical	Loss of service to any designated Key DREN Node or an outage that affects multiple DREN Nodes.
High	Loss of service to a non-Key DREN Node
Enclave	Loss of service supporting a single Subscriber Enclave (including the specific Subscriber outage involving multiple Nodes)
Medium	Any service degradation which does not violate a PWS requirement but does impact Subscriber applications
Low	Any service degradation which does not violate a PWS requirement and does not impact Subscriber applications

Security outage notifications shall be initially via telephone. Upon Government direction, some limited details may be sent out via email (see Section Security Incident Notifications 6.5.5.1.2 Security Incident Notifications). Critical category outage notifications shall be via email, telephone, and text messages. High, medium, and low outage notifications shall occur via email. Update notifications shall occur regularly in accordance with the following table:

Table 6.17 Outage Update Notification Intervals

Outage	Level Required Outage Update Notification Intervals
Security	As directed by the Government
Critical	Hourly
High	Every 4 hours
Enclave	Every 8 hours
Medium	Every 12 hours
Low	Daily

Outage notifications and updates, when via email, shall be via Common Access Card (CAC) signed email and shall follow the Government provided format for outage notifications emails. At a minimum, the notification email shall contain Outage Level, DREN Node/Enclave Name, Ticket Number, Outage and Restoration Time.

When the notification is required via telephone, the Contractor shall contact a DREN staff member via phone Government-provided DREN Emergency Contact Information in the order listed.

Outage notifications and updates, when via text messaging, shall follow the Government provided format for outage notifications sent via text messaging. At a minimum, the notification text message shall contain Outage Level, DREN Node/Enclave Name, Ticket Number, Outage and Restoration Time.

The Contractor shall adjust what types and levels of Notifications are sent, how they are sent, and at what intervals based on direction by the Government.

6.5.5.1.2. Security Incident Notifications

The Contractor shall follow procedures specified in the Contractor's approved Incident Response Plan for issues related to a Security category outage or incident.

Upon initial notification of a Security category outage or incident, the DREN ISSM will provide further guidance as to the classification of the incident, what communication methods and markings will be used for subsequent information exchanges, and other additional personnel to be added to future information exchanges.

6.5.5.1.3. Contractor-Initiated Maintenance Notifications

DREN utilizes four maintenance notification categories: Emergency, Hazardous, Routine, and Advisory as delineated in the table below:

Table 6.18 Maintenance Notification Categories and Notification Requirements

Maintenance Notification Categories	Description
Emergency	Categorized as an event that is required to correct a network problem that would eventually cause a traffic outage if not corrected in a timely manner. DREN Operations will evaluate emergency maintenance requirements. A decision on when to proceed and how to provide notification will be made based on the nature of the network problem.
Hazardous	Categorized as maintenance that may be required in response to: a natural or human-made disaster or adverse condition, activity required to eliminate a threat, or a situation that jeopardizes communications. DREN Operations will evaluate hazardous maintenance requirements, and make a decision on when to proceed and how to provide notification will be based on the nature of the hazardous situation.
Routine	Categorized as periodic network modifications or improvements, Contractor-managed hardware code upgrades, and proactive trouble isolation and resolution that involve any traffic outage. DREN Subscribers shall be notified 14 days prior to the actual maintenance to ensure the maintenance can be coordinated around critical mission events. Be prepared to reschedule routine maintenance at a Subscriber's request

Maintenance notifications from the Contractor to DREN Subscribers shall occur via CAC-signed email and shall follow the Government provided format for maintenance notification emails. At a minimum, the notification email shall contain DREN Node/enclave name, ticket number, maintenance window (with start and end times), and reason for maintenance action.

To prevent any type of focus on potential DREN security weaknesses, the Contractor shall not state a security-related maintenance is being performed, e.g., installing security patches; just simply state that a code upgrade is being performed.

Before the beginning of the maintenance window, the Contractor's Help Desk/NOC shall send a reminder email to the original recipients advising that the maintenance will begin shortly.

Upon completion of any maintenance, ensure a Maintenance Complete notification is transmitted by replying all to the original maintenance notification shall state whether or not the maintenance was completed or not and duration of the service interruption.

6.5.5.1.4. Subscriber-Initiated Maintenance Notifications

Subscriber POCs shall advise the DREN NOC on all scheduled maintenance events that could affect a DREN Node. At a minimum, the DREN site POC shall provide the following information:

a) Maintenance POC

b) Name

c) E-Mail

d) Telephone (Office)

e) Telephone (Mobile)

f) Maintenance Description

g) Affected Site and Enclaves

h) Start Date

i) Start Time (GMT)

j) End Date

k) End Time (GMT)

l) Expected Duration

m) Additional Comments

The Helpdesk/NOC shall open a ticket to track the event when notified of a Subscriber-initiated maintenance that affects the Subscriber's DREN Node. The ticket may be closed upon the completion of the actual maintenance and restoration of service. An email maintenance notification that shall be sent to all DREN Subscribers, using the Government provided notification template. At a minimum, the notification email shall contain the DREN Node/enclave name, Ticket Number, actual start and end times of the maintenance window, and reason for maintenance action.

The DREN Subscriber will coordinate with the Contractor's Helpdesk and DREN Operations, if applicable, immediately prior to the maintenance to allow the graceful shutdown of DREN-deployed equipment. In addition, the DREN Subscriber will contact the Contractor's Helpdesk and DREN Operations, if applicable, immediately after Subscriber-performed maintenance to verify functionality and facilitate troubleshooting by the Contractor's Helpdesk and DREN Operations.

6.5.6. Problem Management

The Contractor shall resolve/correct all reported and non-reported problems affecting the DREN Service as specified in this PWS within the timeframes specified in Table 6.19 Required Repair Times with or without a site visit. Contractor shall perform the following to assist with problem resolution for all identified issues by:

a) providing a list and status of all open trouble tickets upon request by the Government

b) ensuring all issues/problems and actions taken to resolve issues/problems are well-documented in the SMS

c) ensuring status update requirements are met, ticket updates are well documented in the assigned SMS, and outage notification updates are performed as required by this PWS

d) correcting service impacting problems which affect the entire network, or for which there is no standard solution by

   1) developing and documenting individual plans

   2) submitting the plan for Government approval

   3) effecting the correction of each identified problem in accordance with the approved plan

e) providing, when requested by the Government, an After Action Report detailing the cause and resolution of each problem. The Report shall contain the procedural changes, as well as the planned and implemented actions to prevent a re-occurrence of the problem

f) preparing to effect repairs as required in Table 6.19 by completing all installation/facility access requirements for escorted or unescorted personnel to perform an on-site visit and prepositioning assets (both physical and human)

Table 6.19 Required Repair Times

Category	Time Interval
Time to clear problem or issue	30 minutes
Time to on-site visit by field technician (if required): • Key DREN Node locations designated by the Government • DREN Exchange Point (DXP) • All other locations	 4 hours 4 hours 12 hours
Time to clear a problem/issue with an on-site field visit: • Key DREN Node locations designated by the Government • DREN Exchange Point (DXP) • All other locations	 5 hours 5 hours 13 hours

The Contractor shall deliver via the Standard Distribution and no later than the 15th of each month, a Problem Management Report, that documents metrics of Required Repair Times for the previous month. The report shall be in a Contractor defined format and contain at least:

a) Total Number of Trouble Tickets

b) Percentage of problems resolved within the threshold specified in Table 6.19 Required Repair Times

c) Number of problems at key DREN Nodes requiring an on-site visit by a field technician

d) Number of problems at non-key DREN Nodes requiring an on-site visit by a field technician

e) Number of problems at DREN Exchange Points requiring an on-site visit by a field technician

f) Percentage of on-site visits by a field technician to key DREN Nodes performed within the threshold specified in Table 6.19 Required Repair Times

g) Percentage of on-site visits by a field technician to non-key DREN Nodes performed within the threshold specified in Table 6.19 Required Repair Times

h) Percentage of on-site visits by a field technician to DREN Exchange Points performed within the threshold specified in Table 6.19 Required Repair Times

i) Provide the following information for each on-site visit by a field technician that was not performed within the threshold specified in Table 6.19 Required Repair Times

j) Problem Ticket number

k) DREN Node Name

l) The reason the on-site visit was not performed as required

m) Problem Ticket number

n) Total outage time

o) Brief description of the problem

p) Root cause of the problem

q) Resolution of the problem

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.5.6 Problem Management	Problem Resolution /Management	The Contractor meets all requirements specified in this subtask on time and error free	Government review of Problem Management Reports	none

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.6	Problem Management Report	Contractor-Determined Format	15th of each month		Standard Distribution (6.0.2)	Monthly

6.5.7. DREN Node Availability Requirement

The Contractor shall select components and access link quality to ensure each Government accepted DREN Node not experience more than 30 minutes of outage per month.

A Government accepted DREN Node is considered to be in an Outage State when any service ordered in accordance with the terms of this contract specific to a DREN Node are not being provided.

6.5.7.1. DREN Node Outage State Determination

A Government accepted DREN Node is considered in an Outage State when any service ordered in accordance with the terms of this contract specific to a DREN Node is determined to be unavailable, or is being provided at a reduced capability or a degraded condition.

All periods of time that a Government accepted DREN Node is considered to be in an Outage State unless otherwise excluded shall be included in a monthly outage calculation for a DREN Node.

The following times shall not be included in the monthly outage calculation for a Government accepted DREN Node:

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.

d) The first 7200 minutes outages directly resulting from an Act of God.

6.5.7.2. Individual DREN Node MRC Billing Credits

Individual DREN Node Outages shall be calculated based on unavailable minutes. When the unavailable time is 30 minutes or greater, the credit percentage is calculated by

$$AffectedNodeMRC * \min\left\{\frac{(3 * LengthofUnavailability) + 257}{7000}\middle|.5\right\}$$

For example, a node with an MRC of $10000 and an unavailability of 50 minutes the calculation would be:

$$\$10000 * \min\left\{\frac{(3 * 50) + 257}{7000}\middle|.5\right\} = \$10000 * .05814 = \$581$$

The Individual DREN Node MRC Billing Credits are independent from the Adjusted Network Availability (ANA) Total MRC Billing Credit.

6.5.8. Network Availability

The Contractor shall resolve/correct all reported and non-reported problems affecting the availability of DREN Service as specified in this PWS to maintain an Adjusted Network Availability (ANA) of 99.9% or greater for

each month. This measures available end-to-end service time calculated as a percentage of the total time of a month.

6.5.8.1. Adjusted Network Availability (ANA) Determination

The ANA refers to the fraction (or percentage) of total possible uptime achieved in a period. Aggregate Unavailability (AU) refers to the total (qualified) time of service unavailability in minutes aggregated from all DREN Nodes. ANA is calculated by the following industry standard formula, modified to represent the aggregation of all DREN Nodes accepted by the Government in a given month:

$$\text{ANA} = \frac{(\text{Total Availability Possible} - \text{Aggregate Unavailability})}{\text{Total Availability Possible}}$$

The Total Network Availability Possible (TNAP) refers to the total time (in minutes) in a month that the sum of all Government accepted DREN Nodes in the network should be available. This is derived from multiplying the standard number of minutes in a month by the number of Government accepted DREN Nodes. The number of DREN Nodes in service at the end of each month shall be the number of DREN Nodes in the TNAP computation.

$$\text{TNAP} = \text{Number of Minutes in a Month} \times \text{the Number of DREN Nodes}$$

The number of minutes in a month is 43800 minutes based on the following formula:

365 days per year divided by 12 months in a year x 24 hours each day x 60 minutes each hour. In other words,

$$\text{Number of Minutes in a Month} = \frac{365}{12} \times 24 \times 60$$

To calculate AU the following guidelines shall apply:

a) the first 7200 minutes of service outages directly resulting from an Act of God shall not be included in the AU aggregation of service unavailability minutes. Acts of God are considered to be severe outages resulting from:

   1) Tornadic and/or hurricane force destruction, including the associated flooding;

   2) Earthquake destruction;

   3) Other violent acts of nature rendering unusual, inordinate destruction to telecommunication facilities.

b) the first 1080 minutes of any DREN Node outage will not be counted against the ANA.

c) the Contracting Officer or designated representative will be the final arbitrator in allowing the exclusion of Act of God conditions from the ANA computation.

The following is an illustrative computation of the ANA applying the calculation requirements:

A month, equaling a total of 43,800 minutes, ends with 100 DREN Nodes accepted by the Government provides a TNAP of 4,380,000 minutes.

$$\text{Total Network Availability Possible} = 43{,}800 \times 100 = 4{,}380{,}000 \text{ minutes}$$

During the same month, five DREN Nodes experienced service unavailability totaling 7,469 minutes. However, the first 1,080 minutes of outage for each DREN Node is NOT included in the ANA, reducing the aggregate qualified service unavailability by 5,400 minutes, bringing the AU to 2,069 minutes.

In the same month, a sixth DREN Node had an outage due directly to a hurricane, resulting in total of 5,940 minutes of service outage at the affected location. This outage is considered a direct result of an Act of God and therefore is NOT included in the ANA computation.

Because of all outages during the month of this example, the total AU remains at 2,069 minutes. Therefore, the ANA is 0.99953 or 99.953% as illustrated:

$$\text{ANA} = \frac{4{,}380{,}000\ [\text{TNAP}] - 2069\ [\text{AU}]}{4{,}380{,}000\ [\text{TNAP}]} = 0.99953$$

The 99.953% ANA for this illustration is greater than the minimum standard, resulting in no ANA total MRC billing credit for the month.

6.5.8.2. ANA Total MRC Billing Credits

Failure to meet the monthly ANA Requirement of 0.999 (99.9%) shall result in a total MRC billing credit issued by the Contractor.

The Total MRC billing credit shall escalate by one percent for each 1/100% increment whenever the ANA falls below 99.9%. The total MRC billing credits for failure to meet the ANA shall not exceed 50%.

6.5.8.3. Network Availability Report

The Contractor shall produce, by the 15th of each month, the Network Availability Report that shall contain at least the following:

a) For Each DREN Node provide
   1) DREN Node Number
   2) Node Unavailable Minutes
   3) Requested Minutes to be Adjusted including justification (e.g. Acts of God)

b) Total Minutes of all nodes on contract

c) Total Unavailable minutes

d) Network Availability as a percentage

e) Adjusted Network Availability (initially reported with all requested adjusted minutes)

f) Total MRC of all Nodes

g) Computed Network Availability Credit

The Government will review the Report and provide the approved amount of adjusted minutes at which point the Contractor has 5 days to submit a correct revised report. The Contractor shall process credits based on this final report.

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)	
6.5.8 Network Availability	ANA	The Contractor maintains an ANA of 99.9% or greater.	Government review of Network Availability Report	Availability	MRC Plus/Minus
				>=99.9%	0%
				<99.9%	1% for each 1/100% below 99.9 using the formula: $\lfloor (99.9 - ANA) * 100 \rfloor$

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.8	Network Availability Report	Contractor-Determined Format	15th of each month		Standard Distribution (6.0.2)	Monthly

6.5.9. Problem Escalation

The Contractor's Helpdesk shall escalate problems that are beyond its capability, area of responsibility or are not being resolved in required timelines. To facilitate problem resolution for such issues the Contractor shall beginning no later than the commencement of Phase II of the Transition:

a) Develop and deliver with input from the Government, in a Contractor determined format, the Problem Escalation Procedure to include both manual and automated (e.g., trouble ticket system) procedures for escalation to resolution. The Procedure shall reflect methods for coordinating escalations and communications with the Subscribers, and the Government.

b) Review annually and update the Problem Escalation Procedure when changes occur.

c) Develop, implement and maintain an escalation function within the trouble ticket system to support automated escalation of unresolved problems, including, the generation of e-mail messages to the Government and the designated DREN Subscriber site POCs when a trouble ticket is escalated.

d) Ensure the ticket system has the current list of personnel within the Contractor's Organization and their contact information (at least their job/function title, email, phone, and cell number if provided).

e) Ensure the ticket system has the current list of DREN Subscriber personnel and their contact information (at least their job/function title, email, phone, and cell number if provided) for each DREN Node and Subscriber Enclave. The list of personnel shall contain the following DREN POC types:

1) Primary and Alternate POCs

2) After-hours POC(s)

3) Security Manager(s)

4) Other POC(s), as specified by the Government

f) Document in the trouble ticket the name of the last person contacted and the time of contact, the name and job/function title of the next person in line to be contacted, and the projected time for that next contact.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.9	Problem Escalation Procedure	Contractor-Determined Format	Prior to IPC Demonstration		Standard Distribution (6.0.2)	One time, changes reviewed annually

6.5.10. Data Access and Storage Requirements

The Contractor and Government will be exchanging data throughout the DREN4 contract. Some of this data will be hosted by the Government (e.g., CDRLs), while other data will be hosted and maintained by the Contractor (e.g., Network Utilization Reports). The specific requirements of each follow.

6.5.10.1. DREN Network Dynamic Data

The Contractor shall provide tools for the Government and Subscribers to access information about the DREN Network and its operations in real time.

The Contractor shall:

a) Establish a secure web-based Dynamic Data Site (including at least the Dashboard, Looking Glass and Flow Tool) prior to the IPC Demonstration as a component of the SMS.

b) Provide data access controls such that groups of individuals can be granted access to or restricted from sets of data (e.g., access to site specific data by registered DREN POCs) as directed by the Government.

c) Ensure that access and authorization is controlled through the use of DoD PKI

d) Ensure that all data exchanges with back-end system(s), if any, are encrypted.

e) Ensure that all data collected is stored and maintained to be available to the Government throughout the life of the contract, unless otherwise specified.

6.5.10.1.1. API

The Contractor shall provide an Application Programming Interface (API) for the Government to access all DREN latency and utilization that the Contractor records. The interface shall also provide machine-to-machine direct data access with structured data responses

The Contractor shall ensure the API meets the following requirements, at a minimum:

a) accessible by Government systems on DREN (specifics to be provided after Contract award)

b) supports encryption for data in transit

c) supports filtering of data sets on a per request/query basis on at least the following criteria:

1) DREN Node(s)

2) DREN Node port(s) (N/A for latency data)

3) date ranges

The Contractor shall provide the API documentation (e.g., any data structures, routines, variables) to the Government to facilitate usage and implementation.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.10.1.1	API Documentation	Contractor Determined Format	Beginning of IPC Demonstration		Standard Distribution (6.0.2)	One time, updated within 15 days of API changes

6.5.10.1.2. Looking Glass

The Contractor shall provide a Looking Glass with the following capabilities:

a) perform and display on demand the results of IPv4 and IPv6 pings and traceroutes between any Contractor-deployed DREN system and another DREN system or a user-specified IP address

b) perform and display on demand the results of Ethernet delay and path tests between any Contractor-deployed DREN system and another DREN system or a user-specified MAC address

c) perform and display on-demand the results of user-entered queries to determine if traffic would be blocked (e.g., ACL, firewall) by any Contractor-deployed DREN networking systems. The queries shall support both inbound and outbound directions and the specification of source and/or destination IP or MAC address(es)

d) perform and display on-demand the results of queries to validate that a whitelist exception is in place on all Contractor-deployed DREN networking systems where such whitelist controls are applied. The queries shall support specification of the protocol (e.g., HTTPS [Hypertext Transfer Protocol Secure], IPsec) and destination IP address

e) display on-demand the results of Government specified "show" commands on a singular or simultaneously on multiple Contractor-deployed DREN networking system(s), and if the user chooses, search the output using a user-defined regular expression

f) provide on-demand a report of DREN Node interface port allocations mapped to IP address and VLAN allocations as well as advertised ASNs and IP prefixes

g) display on-demand BGP route reports for any DREN received, accepted, and advertised BGP route table or DREN BGP community

6.5.10.1.3. Data Dashboard

The Contractor shall deploy a Data Dashboard with at least the following capabilities:

a) Node Summary Report to include at minimum:
   1) Node Number
   2) Node Name
   3) Physical Location (City, State or Post, Camp, Station Identifier)
   4) DREN Node Line Rate
   5) Status (up/down/degraded)
   6) Count of open tickets

b) In the Node Summary Report the capability should exist to expand the details of a DREN Node to include at a minimum:
   1) for SDPs the list of Subscriber Enclaves and their interface details
   2) for DXPs the list of external peers and their details (BGP information, interface details, cross connect or intermediate party details)
   3) tickets affecting the Node (open and closed)

c) provide a real-time DREN Node report of status and reachability between Nodes (sometimes referred to as a weather map)

d) provide on-demand Utilization Reports by interface for all Contractor-deployed DREN networking systems; in graphical format; and, ensure data required to support Utilization Reports is maintained for at least one year

e) provide on-demand Latency, Jitter, and Packet Loss Reports (each its own) and ensure that data required to support these reports are maintained for at least one year. The report generation shall support the following selections
   1) among all, or between selected individual DREN Nodes
   2) daily or monthly
   3) full data or average/min/max
   4) graphical or raw data (.csv format)

f) provide a real-time report of IP address and VLAN allocations from the 6.5.4 Contractor Managed Network Database

g) provide on-demand the daily configuration snapshot from any DREN networking system. The query shall support selection of any daily snapshot for at least the past 30 days. The query shall support showing the differences between any two selected snapshots

The exact format and data included in the dashboard shall be coordinated with the Government to the mutual benefit of both the Government and the Contractor.

6.5.10.1.4. Flow Tool

The Contractor shall collect and store all data required to produce flow data reports. This data shall be maintained for at least one year. The Contractor shall implement a system to display on-demand, the following types of flow data reports from all Contractor-deployed DREN network components in graphical and raw data (.csv) format:

a) top sources, destinations, or session by amount of data

b) top source, or destination AS

c) top ports or protocols

6.5.10.2. Government Documentation Repository

The Government will provide a system that the Contractor shall use for submission of CDRLs and other documentation pertaining to the management or execution of the DREN4 contract. The Government will provide instructions including naming and placement, and DoD PKI access to the system following contract award.

The Contractor shall:

a) Ensure that the all Contract Data Requirements List (CDRL) items are submitted to this Government Documentation Repository by their due dates.

b) Notify designated Government personnel, via email, when CDRLs are available in the Government Documentation Repository.

c) Submit to the Government Documentation Repository copies of approved TIPs, and with all accompanying documentation.

d) Ensure that all other documentation pertaining to the management or execution of the DREN4 contract is maintained in the Government Document.

e) Follow the naming and placement instructions provided by the Government.

6.5.11. OOB Access

The Contractor shall:

a) Implement POTS modem based secure Out-of-Band (OOB) capability on all Contractor-deployed DREN Node systems and maintain the access throughout the life of the contract. The capability shall include at minimum all components necessary to restore in-band management network access to the Node.

b) Validate OOB access weekly and prior to any maintenance event on a Node

c) Repair all OOB access failures within one week.

d) Deliver a weekly OOB Status Report in a Microsoft Office Excel format via Standard Distribution weekly by each Thursday at 12:00, Eastern Time that contains at least the following information:

1) DREN Node Number as designated by the Government
2) DREN Node Name as designated by the Government
3) POTS Number
4) Date Tested
5) Status: Pass/Fail
6) Fail Reason
7) Actions being taken to resolve failure

e) Utilize the following naming convention for weekly OOB Status Reports: OOB Status Report yyyymmdd

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.5.11 OOB Access	OOB Access Function	The Contractor deploys and maintains an OOB Access capability, performs OOB Access Testing weekly and repair failures within a week	Government review of OOB Status Reports	None

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.11	OOB Status Report	Microsoft Office Excel spreadsheet with Contractor determined layout	Weekly by each Thursday at 12:00, Eastern Time		Standard Distribution (6.0.2)	weekly

6.5.12. Regression Testing

Regression testing of new versions of DREN systems software and/or hardware prior to deployment is vital to the sustainment of DREN. Therefore, the Contractor shall:

a) Perform regression testing on new software and/or hardware prior to use on DREN to validate that current features, functions, and capabilities that support the services provided meet or exceed requirements and enhancements that support new features, functions, or capabilities perform/operate properly.

b) Develop a Regression Test Plan and Regression Test Report to validate the operability of all features, functions and capabilities utilized in a vendor's software and/or hardware to support all current services provided. The Regression Test Plan shall contain at least the following information:

1) Title

2) Date

3) Revision Number

4) Table of Contents

5) List of Tables

6) List of Figures

7) Record of Change

8) Introduction to contain:

   A) The reason for the regression test

   B) Issues to be resolved using the new software and/or hardware

   C) Desired/Enhanced Features/Capabilities of the new software and/or hardware

9) Test topology with detailed physical and logical flow diagram

10) List of devices under test to include version under test

11) Individual test of each feature, function, or capability either currently utilized or being added on DREN to include a test name, required test actions, the expected results, the pass/fail criteria

12) In addition the Report (which may be incorporated into the Plan document) shall also contain:

13) actual results

14) pass/fail indicator

c) Develop a software upgrade Method of Procedure (MOP) to include the following:

1) Pre-installation procedures

   A) Procedures for performing a system backup

   B) Procedures for performing OOB communications check

   C) Software installation procedures

2) Post-installation procedures

   A) Procedures for activating the new software

   B) Procedures to validate functionality of all Subscriber services

3) Upgrade Failure Procedures

   A) Procedures for determining when to abort the upgrade process and downgrade due to a software upgrade failure

   B) Procedures for performing a downgrade due to a software upgrade failure

   C) Procedures for restoring service in the event of an upgrade or hardware failure

4) Quality Assurance (QA) processes, procedures, activities and checklists necessary to ensure an error free software upgrade

d) Develop an Upgrade Schedule for each upgrade, to include the following:

1) DREN Node Number
2) DREN Node Name
3) Device(s) to be upgraded
4) OOB Access Number
5) Planned Upgrade Date
6) Alternate Upgrade Date

The Government will review all draft documents, and provide comments and recommendations.

Upon receipt of Government feedback, the Contractor shall have seven days to incorporate updates to the document and provide the final version.

The Contractor shall seek Government approval (6.3.2 Configuration Control Board Change Requests) to deploy after review of the Regression Test Report, the MOP and the Upgrade Schedule by the Government.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.12	Regression Testing Plan	Contractor-Determined Format	15 days after regression testing ticket opened		Standard Distribution (6.0.2)	As required
	Regression Test Report		Seven days after regression testing is complete			
	Change/upgrade MOP		Seven days after regression testing is complete			
	Upgrade Schedule		Seven days after regression testing is complete			

6.5.13. DREN Node Documentation

6.5.13.1. DREN Node Master Plan

The Contractor shall:

a) Deliver a DREN Node Master Plan as specified in DREN Node Master Plan Template

b) Deliver a draft DREN Node Master Plan within 90 days after contract award and posted via Government Documentation Repository. Upon Government receipt of the draft DREN Node Master Plan, the Government will respond with comments and recommendations.

c) Submit a proposed Final DREN Node Master Plan within 15 days of receiving comments and recommendations from the Government electronically and posted via Standard Distribution

d) Update, revise, and maintain the DREN Node Master Plan throughout the life of the contract.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.13.1	DREN Node Master Plan	DREN Node Master Plan Template	Draft version 90 days after contract award; final version 15 days after receiving comments and recommendations from the Government		Standard Distribution (6.0.2)	One time, and updated as necessary after

6.5.13.2. Individual DREN Node As-Built Reports

The Contractor shall:

a) Deliver an Individual DREN Node As-Built Report in a Contractor-determined format that addresses site-specific details, via the On-Line Data Repository, within seven days upon Government acceptance of a new or upgraded DREN Node. The report shall include the following information:

1) Title
2) DREN Node Name
3) DREN Node Number
4) Date of Individual DREN Node As-Built Report
5) Revision Number
6) Table of Contents
7) List of Tables
8) List of Figures
9) Record of Change
10) Any variance from the standards documented in the approved DREN Node Master Plan and incorporated elements and applicable wiring, electrical, HVAC, construction and related standards.
11) The exact location of the DREN Node (physical address to include building and room number)
12) Floor Plan that includes any enclosures or restrictions, e.g., cage, locking cabinet, and floor space, etc., bearing on Contractor and (non-end-user) Government deployed hardware.
13) Rack Elevation view drawing of the equipment rack(s) or cabinet(s) in which the Contractor and (non-end-user) Government deployed hardware installed

14) Rack face diagram for each hardware component deployed by the Contractor

15) Power/Grounding Running List

16) POTS Line Number

17) Bill of materials at the major end item level for all Contractor-deployed hardware

18) System Wiring Diagram that documents the physical connectivity between the access link provider's demarcation point and Contractor-deployed hardware. A diagram documenting the physical connectivity between the POTS delivery point and the Contractor-provided out-of-access modem should also be provided.

19) A port list that documents all the port numbers and connection and media type for all Contractor-deployed hardware

20) The results of the satisfactorily complete DREN Node Acceptance Test.

b) Ensure that all embedded objects, such as diagrams and images, can be opened and are legible.

c) Deliver an updated Individual DREN Node As-Built Report via the Standard Distribution within seven days of any completed and Government-accepted change to a DREN Node.

d) Ensure that individual DREN Node Plans are maintained for the life of the contract.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.13.2	Individual DREN Node As-Built Report	Contractor-Determined Format	Seven days after Government acceptance of a new or upgraded DREN Node		Standard Distribution (6.0.2)	As required

6.5.13.3. DREN Node Site Survey Template

The Contractor shall develop a draft DREN Node Site Survey Template in a Contractor-chosen content format and provide it to the Government electronically 21 days after contract award.

Upon receipt of Government DREN Node Site Survey Template comments and recommendations, the Contractor shall:

a) Submit a Final DREN Node Site Survey Template via the Government Documentation Repository within 21 days.

b) Update, revise, and maintain the DREN Node Site Survey Template throughout the life of the contract.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.13.3	DREN Node Site Survey Template	Contractor-Determined Format	Draft: 21 days after contract award Final: 21 days after Government feedback on draft Within seven days of any significant change		Standard Distribution (6.0.2)	One time, update as required

6.5.13.4. DREN Node Site Surveys

Upon execution of a DITCO-issued service order issued by the Contracting Officer, or other designated authorized representative, the Contractor shall:

a) Conduct, as necessary, one or more site surveys, at no additional cost to the Government, within 30 days, to identify the availability of facilities, materials, and equipment; verify Subscriber requirements; and, provide cost and completion date estimates.

b) Conduct, as necessary, one or more site surveys, at no additional cost to the Government, within 21 days of service termination to identify equipment and/or cabling that shall be removed and any that shall be abandoned in place.

c) Coordinate with the organization responsible for the facility in which the DREN Node is to be installed and the access link provider(s) to identify and document any site readying requirements, e.g., environmental (security, HVAC, airflow), electrical power, grounding, size/space, etc., that must be addressed to support delivery of the local access link and installation of the SDP.

d) Obtain copies of any access link provider(s) notifications, e.g., letters or EUCR (End User Contingency Requirements) forms and ensure they are incorporated in, or attached to, the site survey, and that they are provided to the local DREN POC, the organization responsible for the facility, and DREN Operations, in conjunction with the site survey report or upon its receipt.

e) Deliver all Site Survey Reports via the Standard Distribution and the local DREN POC electronically within seven days of completion of a site survey visit with the exception of those site surveys conducted prior to the IPC demonstration. Site surveys conducted prior to the IPC demonstration may initially be delivered to the Government and local DREN POC electronically and posted via the Standard Distribution, when it becomes available.

f) Notify the new/existing DREN end-user 14 days prior to the date of a requested visit.

g) Have flexibility in performing site surveys to accommodate end-user availability.

h) Complete all installation/facility access requirements for escorted or unescorted access to perform a site survey.

i) Not proceed beyond the site survey requirement without authorization from the Government.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.13.4	DREN Node Site Survey	Contractor-Determined Format	30 + seven days after DITCO issues service order for new/change 21 + seven days after DITCO issues service order for termination		Standard Distribution (6.0.2)	As required

6.5.13.5. DREN Node Location Modification Plan

In the event that a facility change or modification is required to support the installation or upgrade of a DREN Node, the Contractor shall:

a) Provide a description of required changes for each DREN Node Location modification or upgrade action and ensure the description addresses the following:

1) Transmission media construction such as cabling, repeaters, and conduits.

2) Building modifications, if any, necessary to install equipment and run cables.

3) Storage space requirements.

4) Staging area requirements.

5) An analysis of the impact on the active DREN Node at the site requiring the modification and at other sites, including identification of any actions needed to prevent negative impact.

b) In the event further site survey is required, contact the Government-identified Site End-User at least 14 days prior to the survey to schedule the visit.

c) Deliver via the Standard Distribution within 14 days after delivery of DREN Node Site Survey for the given location.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.13.5	DREN Node Location Modification Plan	Contractor-Determined Format	14 days after delivery of DREN Node Site Survey		Standard Distribution (6.0.2)	As required

6.5.14. Acceptance Testing

6.5.14.1. Acceptance Test Plan

When a new DREN Node is ordered, the Contractor shall validate the proper installation and operation of a DREN Node with its ordered services and interfaces in accordance with the approved Acceptance Test Plan.

The objective is to ensure that an ordered DREN Node with one or more interfaces and one or more separately orderable functions is correctly configured and is compliant with DREN service requirements. Successful testing in accordance with the approved Plan will result in an "active" DREN Node with services and interfaces that meet the requirements specified in this PWS.

The Contractor shall develop an Acceptance Test Plan, prior to IPC demonstration, that validates packet loss, network latency, TCP throughput, network throughput and add on functions satisfy the requirements specified in this PWS. The Acceptance Test Plan shall:

a) identify all Contractor provided reference test points on the DREN network including their physical locations, configurations and capabilities

b) identify all applications, test equipment, and other hardware required at each of the reference test points

c) describe the signal flow(s) between the DREN Node under test and the reference test points that are utilized during testing

d) describe pre-test preparation steps and actions required

e) describe the actual acceptance test steps, to include a test description, test procedure, expected results, and a pass/fail criterion for each test step

f) identify the location(s) and personnel involved in acceptance testing and identify conditions under which the Local site personnel are required to assist the Contractor in testing

g) describe initial acceptance testing of a DREN Node and testing conducted to accept an upgrade to, new service ordered for, or new function added to an existing DREN Node, to include personnel, applications, test equipment and other hardware involved in each

h) specify the information to be included in the report to be generated for each DREN Node under test.

i) Include a table detailing each test to be performed, the PWS reference and description for each characteristic of a service, interface and function to be tested

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.14.1	Acceptance Test Plan	Contractor-Determined Format	Prior to IPC Demonstration		Standard Distribution (6.0.2)	One time, update as required

6.5.14.2. Acceptance Test Report

The Contractor shall submit an Acceptance Test Report for each DREN Node as part of an Individual DREN Node As-Built Report within seven days following satisfactory testing. At a minimum, the Acceptance Test Report shall include:

a) date and time of testing

b) reference test point(s)

c) name of the DREN Node under testing

d) the latitude and longitude of the DREN Node under testing

e) line-of-sight (LOS) distance in kilometers between the reference test point(s) and the DREN Node under testing

f) type of service(s), interface(s), and function(s) tested

g) test equipment and applications used

h) service performance: latency, jitter, TCP, throughput, and packet loss

i) metrics captured

j) contractor personnel that performed the testing

k) government witness(es) of the testing

For all acceptance tests, the Government reserves the following rights:

a) to witness any DREN Node Acceptance Test

b) to delay the start of the DREN Node Acceptance Test, at no additional cost to the Government, but such delay will not exceed three days

c) to require the Contractor to rerun, at no additional cost to the Government, any or all portions of the DREN Node Acceptance Test in the event that the DREN Node fails to pass any of the test criteria

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.5.14.2	Acceptance Test Report	Contractor-Determined Format	Seven days following satisfactory testing		Standard Distribution (6.0.2)	As required

6.5.14.3. Acceptance Procedures

Following installation of a DREN Node, the Contractor shall execute acceptance testing in accordance with the Government-approved DREN Node Acceptance Testing Plan (6.5.14.1 Acceptance Test Plan)

6.5.14.4. Tools and Test, Measurement, and Diagnostics Equipment (TMDE)

The Contractor shall provide state-of-the-art tools and test equipment to support the requirements identified in this PWS. The Contractor shall ensure that all Contractor-owned or leased test equipment is calibrated in accordance with manufacturer's specifications.

6.5.15. DNS Service

The Contractor shall implement and maintain a hidden master for DNS resource records. The Contractor shall be responsible for the core.dren.net domain (or its replacement) and PTR records for all IP segments assigned for use by the Contractor. Government systems will act as the authoritative servers for all of these zones. The Contractor shall establish, together with the Government, appropriate network and DNS architecture and

configuration to effect zone transfers in a standards and security compliant manner. The Contractor shall accurately register all DNS records and maintain the records on a continuous basis (24x7x365).

The Contractor shall update DNS records any time the network is changed. The contractor shall ensure all changes to DNS are fully effected and accurate within 2 hours.

The Contractor shall take over management of any existing DREN III master zone files that the Government identifies will continue to be used during the DREN4 contract. This migration will occur in stages during the transition period.

The Contractor shall implement DNSSEC on all master zones they are required to maintain. The Contractor shall coordinate publishing of DNSSEC information to the parent zones with the Government.

The Contractor shall coordinate with the Government to design and apply a subordinate zone naming schema in conjunction with the DREN Addressing Plan. The Contractor shall coordinate adjustments and exceptions to the schema with the Government.

The Contractor shall implement an auditing methodology to identify and fix any missing or inaccurate DNS records. The Contractor shall provide as part of the 6.4.1.8 Program Management Review (PMR) a report of the changes, accuracy, and timeliness of DNS record management.

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.5.15 DNS Service	Accurate DNS Resource Records	The Contractor immediately updates records to reflect changes and continuously audits the DNS records and maintains 100% accuracy	Monthly report (6.4.1.8) of changes and auditing of DNS records missing or inaccurate	70% to<90% -2% NOC MRC <70% -10% NOC MRC

6.5.16. Touch Labor

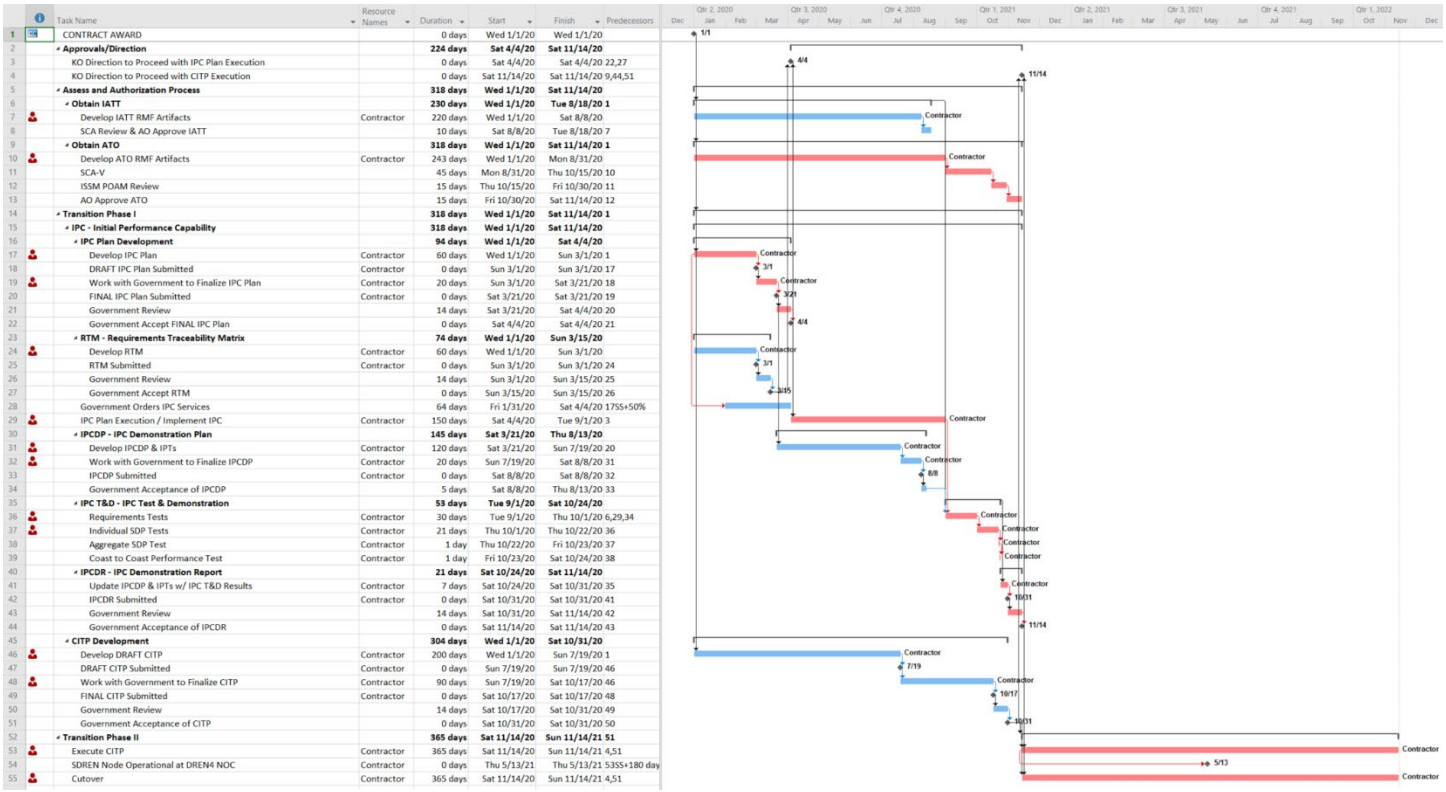
Touch labor is defined as any labor that requires going to a piece of equipment to check its status or perform a physical change. This can include but is not limited to verifying power status or network connectivity, installing or replacing Government provided equipment or components, connecting cables, connecting hosts to equipment management ports, and other interactions that require physical contact with equipment. The Contractor shall provide as ordered by the Government.

6.6. Implementation and Transition

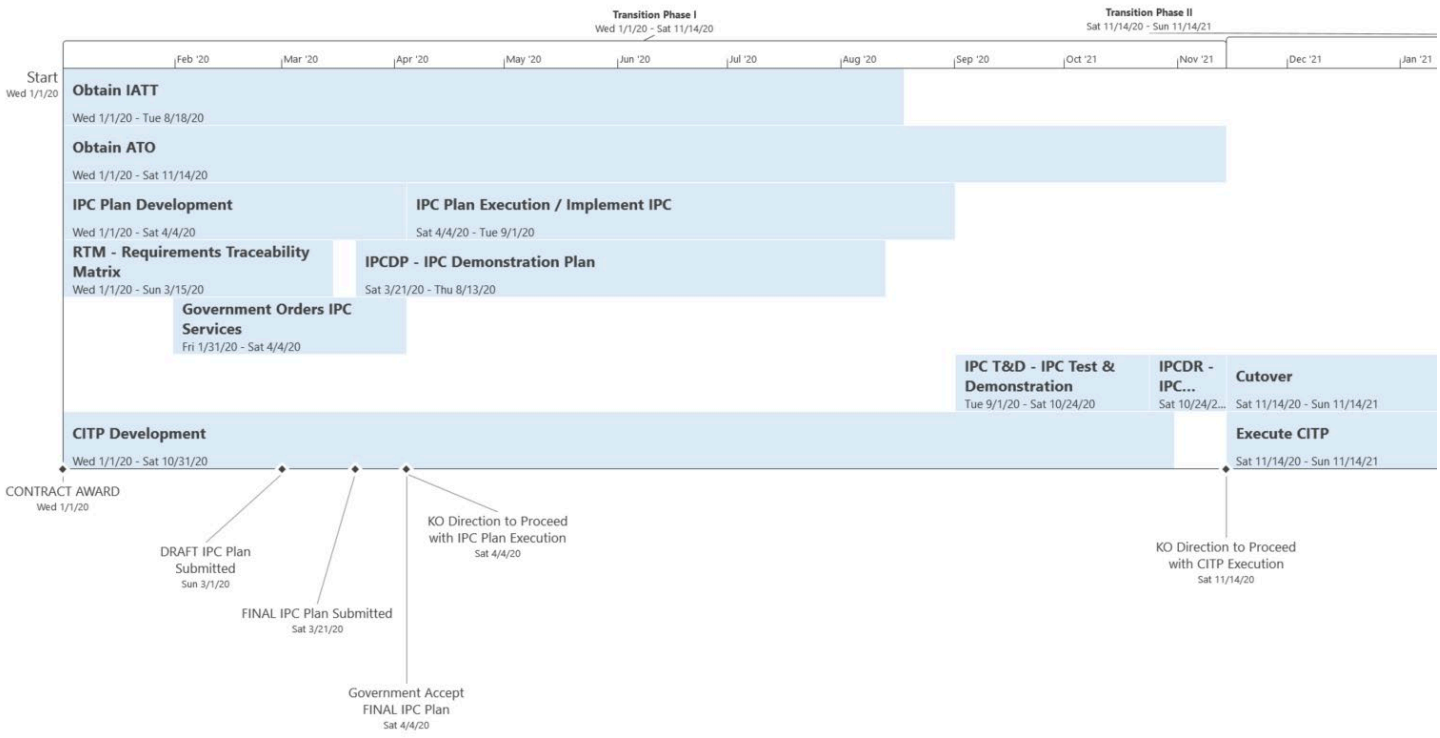
The Contractor is responsible for all necessary planning and actions to successfully implement DREN4 and transition the existing DREN III sites to DREN4. This will be completed in two phases: Phase I shall primarily consist of the implementation and testing of the IPC; Phase II shall consist of the execution of the CITP and cutover of all DREN Subscribers to DREN4.

During IPC, the Contractor demonstrates its ability to meet PWS requirements by implementing a subset of the overall DREN4 network. CITP documents the Contractor's plan to implement the remainder of the DREN4 network following IPC, and cutover of existing DREN III sites and Subscribers.

There are many concurrent activities and deliverables during Phase I that must be efficiently executed by the Contractor. Performance in accordance with the schedule during both Phase I and Phase II will be closely monitored by the Government. The Contractor shall coordinate closely with the Government throughout Phase I and Phase II to minimize schedule impacts. The following high-level timeline and Gantt chart are provided as an illustration of the timeline, dependencies, and concurrent activities. NOTE: The actual dates used are for illustrative purposes only; the focus should be on the dependencies and durations. The Contractor may use these to assist in the planning and execution of both Phases I and II. The Contractor has the flexibility to adjust as appropriate, as long as all requirements (e.g., milestones) in the PWS are met or exceeded. Effective communication with the Government and early submission of all plans and other deliverables will help ensure the Contractor successfully completes transition within the required timeline.



	Task Name	Resource Names	Duration	Start	Finish	Predecessors
1	CONTRACT AWARD		0 days	Wed 1/1/20	Wed 1/1/20	
2	**Approvals/Direction**		**224 days**	**Sat 4/4/20**	**Sat 11/14/20**	
3	KO Direction to Proceed with IPC Plan Execution		0 days	Sat 4/4/20	Sat 4/4/20	22,27
4	KO Direction to Proceed with CITP Execution		0 days	Sat 11/14/20	Sat 11/14/20	9,44,51
5	**Assess and Authorization Process**		**318 days**	**Wed 1/1/20**	**Sat 11/14/20**	
6	**Obtain IATT**		**230 days**	**Wed 1/1/20**	**Tue 8/18/20**	**1**
7	Develop IATT RMF Artifacts	Contractor	220 days	Wed 1/1/20	Sat 8/8/20	
8	SCA Review & AO Approve IATT		10 days	Sat 8/8/20	Tue 8/18/20	7
9	**Obtain ATO**		**318 days**	**Wed 1/1/20**	**Sat 11/14/20**	**1**
10	Develop ATO RMF Artifacts	Contractor	243 days	Wed 1/1/20	Mon 8/31/20	
11	SCA-V		45 days	Mon 8/31/20	Thu 10/15/20	10
12	ISSM POAM Review		15 days	Thu 10/15/20	Fri 10/30/20	11
13	AO Approve ATO		15 days	Fri 10/30/20	Sat 11/14/20	12
14	**Transition Phase I**		**318 days**	**Wed 1/1/20**	**Sat 11/14/20**	**1**
15	**IPC - Initial Performance Capability**		**318 days**	**Wed 1/1/20**	**Sat 11/14/20**	
16	**IPC Plan Development**		**94 days**	**Wed 1/1/20**	**Sat 4/4/20**	
17	Develop IPC Plan	Contractor	60 days	Wed 1/1/20	Sun 3/1/20	1
18	DRAFT IPC Plan Submitted	Contractor	0 days	Sun 3/1/20	Sun 3/1/20	17
19	Work with Government to Finalize IPC Plan	Contractor	20 days	Sun 3/1/20	Sat 3/21/20	18
20	FINAL IPC Plan Submitted	Contractor	0 days	Sat 3/21/20	Sat 3/21/20	19
21	Government Review		14 days	Sat 3/21/20	Sat 4/4/20	20
22	Government Accept FINAL IPC Plan		0 days	Sat 4/4/20	Sat 4/4/20	21
23	**RTM - Requirements Traceability Matrix**		**74 days**	**Wed 1/1/20**	**Sun 3/15/20**	
24	Develop RTM	Contractor	60 days	Wed 1/1/20	Sun 3/1/20	
25	RTM Submitted	Contractor	0 days	Sun 3/1/20	Sun 3/1/20	24
26	Government Review		14 days	Sun 3/1/20	Sun 3/15/20	25
27	Government Accept RTM		0 days	Sun 3/15/20	Sun 3/15/20	26
28	Government Orders IPC Services		64 days	Fri 1/31/20	Sat 4/4/20	17SS+50%
29	IPC Plan Execution / Implement IPC	Contractor	150 days	Sat 4/4/20	Tue 9/1/20	3
30	**IPCDP - IPC Demonstration Plan**		**145 days**	**Sat 3/21/20**	**Thu 8/13/20**	
31	Develop IPCDP & IPTs	Contractor	120 days	Sat 3/21/20	Sun 7/19/20	20
32	Work with Government to Finalize IPCDP	Contractor	20 days	Sun 7/19/20	Sat 8/8/20	31
33	IPCDP Submitted	Contractor	0 days	Sat 8/8/20	Sat 8/8/20	32
34	Government Acceptance of IPCDP		5 days	Sat 8/8/20	Thu 8/13/20	33
35	**IPC T&D - IPC Test & Demonstration**		**53 days**	**Tue 9/1/20**	**Sat 10/24/20**	
36	Requirements Tests	Contractor	30 days	Tue 9/1/20	Thu 10/1/20	6,29,34
37	Individual SDP Tests	Contractor	21 days	Thu 10/1/20	Thu 10/22/20	36
38	Aggregate SDP Test	Contractor	1 day	Thu 10/22/20	Fri 10/23/20	37
39	Coast to Coast Performance Test	Contractor	1 day	Fri 10/23/20	Sat 10/24/20	38
40	**IPCDR - IPC Demonstration Report**		**21 days**	**Sat 10/24/20**	**Sat 11/14/20**	
41	Update IPCDP & IPTs w/ IPC T&D Results	Contractor	7 days	Sat 10/24/20	Sat 10/31/20	35
42	IPCDR Submitted	Contractor	0 days	Sat 10/31/20	Sat 10/31/20	41
43	Government Review		14 days	Sat 10/31/20	Sat 11/14/20	42
44	Government Acceptance of IPCDR		0 days	Sat 11/14/20	Sat 11/14/20	43
45	**CITP Development**		**304 days**	**Wed 1/1/20**	**Sat 10/31/20**	
46	Develop DRAFT CITP	Contractor	200 days	Wed 1/1/20	Sun 7/19/20	1
47	DRAFT CITP Submitted	Contractor	0 days	Sun 7/19/20	Sun 7/19/20	46
48	Work with Government to Finalize CITP	Contractor	90 days	Sun 7/19/20	Sat 10/17/20	46
49	FINAL CITP Submitted	Contractor	0 days	Sat 10/17/20	Sat 10/17/20	48
50	Government Review		14 days	Sat 10/17/20	Sat 10/31/20	49
51	Government Acceptance of CITP		0 days	Sat 10/31/20	Sat 10/31/20	50
52	**Transition Phase II**		**365 days**	**Sat 11/14/20**	**Sun 11/14/21**	**51**
53	Execute CITP	Contractor	365 days	Sat 11/14/20	Sun 11/14/21	4,51
54	SDREN Node Operational at DREN4 NOC	Contractor	0 days	Thu 5/13/21	Thu 5/13/21	53SS+180 day
55	Cutover	Contractor	365 days	Sat 11/14/20	Sun 11/14/21	4,51



6.6.1. Phase I

During Phase I of Implementation and Transition, the Contractor shall:

d) Develop the IPC Plan

e) Develop the Requirements Traceability Matrix (RTM)

f) Implement IPC following the IPC Plan

g) Develop the IPC Demonstration Plan (IPCDP)

h) Execute the IPC Test and Demonstration

i) Update the IPCDP with the results of the IPC Test and Demonstration and deliver an IPC Demonstration Report (IPCDR)

j) Support the RMF Subtasks in pursuit of an IATT (6.3.1.1 RMF IATT Package) and ATO (6.3.1.2 RMF ATO Package)

k) Develop the CITP

There is no entrance criteria to Phase I. The Contractor shall begin the planning and execution of Phase I activities immediately upon contract award.

Phase I shall be completed no later than 318 days after contract award. The exit criteria for Phase I is the acceptance of the IPCDR and the final CITP by the Contracting Officer.

6.6.1.1. Initial Performance Capability (IPC)

The IPC will demonstrate and prove the Contractor's process for the installation and testing of an initial set of DREN Nodes, as well as the initial ramp-up of other capabilities and requirements such as the NOC, security services, and the RMF process.

During IPC, the Contractor shall implement and test a subset of the DREN network and services, restricted only by what the Government orders as a part of IPC. The remainder of the testable requirements from the PWS will be deferred until later in the contract if/when the Government orders the CLIN(s) required to support those untested services. The services ordered as a part of IPC are intended to be active for the life of the contract or until the Government issues a termination order (i.e., IPC infrastructure and services remain following IPC and is the basis for the rest of DREN4).

While the precise set of services delivered will depend on what the Government orders for IPC, the Government expects that IPC will consist of at least the following:

l) The fully implemented6.5.5 Network Operations Center (NOC)

m) Initial integration with HPC CSSP services, such as ACAS and HBSS

n) Three initial DCNs

   1) The location and DREN Node Line Rate of these three initial DCNs are based on the Contractor's application of the DCN optimization methodology (6.1.3.5 DCN Placement)

   2) Two of these DCNs will also function as Tunnel Termination Points (TTPs) for the SDP-L Nodes

o) 15 initial DREN Nodes from the following table (one from each line)

Name	Line Rate	Node Type
sandiego	100Gbps	SDP[1]
wpafb	100Gbps	SDP[1]
equinix-iad	2x10Gbps	DXP
drfortress-hnl	10Gbps	DXP
paxriver or redstone or nrl-dc	10Gbps	SDP
offutt or usafa or dpg	1Gbps	SDP
keyport or ftgreely	1Gbps	SDP
rome or hanscom or hanover	1Gbps	SDP
eglin or charleston or ftgordon	1Gbps	SDP
fthood or wsmr or kirtland	1Gbps	SDP
sdp-lite-1[2]	N/A	SDP-L
sdp-lite-2[2]	N/A	SDP-L
dcn-1	TBD[3]	DCN
dcn-2	TBD[3]	DCN
dcn-3	TBD[3]	DCN

[1]Also will serve as transition gateway between DREN III and DREN4.

[2]Physical address and network connection details will be provided to Contractor upon award

[3]Line Rate determined by the Government based on the Contractor's application of the DCN optimization methodology (6.1.3.5 DCN Placement)

p) Internet Transit Service (ITS) on at least one of the DCNs or DXPs (6.1.2.11 Internet Transit Service (ITS) (Separately Orderable))

q) Large Generic Compute Function (6.2.4.1 Generic Compute Function), Large Firewall Function (6.2.3 Firewall Function (Separately Orderable)), and Large DJS Compute Function (6.2.4.3 DJS Compute Function) on at least one DCN

r) One Large and One Medium Router Function and One Medium-Plus Router Function on the DCNs (6.2.2 Router Function (Separately Orderable))

6.6.1.1.1. IPC Plan

The Contractor shall develop an IPC Plan that includes the following, at a minimum:

a) The Contractor's high-level technical approach to meeting all of the objectives of IPC (6.6.1.1 Initial Performance Capability (IPC))

b) The Contractor's detailed method of implementation for IPC, including timelines, dependencies, and order of operations

c) The Contractor's known risks to a successful IPC using a risk quadrant chart for each risk

The Contractor shall submit draft IPC Plan revisions to the Government during the first 60 days after contract award. The Government will then review the details of the plan and work with the Contractor to finalize the IPC Plan for the next 20 days. The Contractor shall then submit the final IPC Plan.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.6.1.1.1	IPC Plan	Contractor-Determined Format	Draft version 60 days after contract award; final version 80 days after contract award		Standard Distribution (6.0.2)	One time

6.6.1.1.2. Requirements Traceability Matrix (RTM)

The Contractor shall develop an RTM. The RTM will be a living document throughout the DREN4 contract.

The Contractor shall include in the RTM the following, at a minimum:

a) All requirements of the PWS, identifying the following elements of each:

1) Requirement ID

2) Title/Name

3) Summary

4) Detailed Description

5) PWS Section(s)

6) CLIN(s), if applicable

7) Individual Performance Test (IPT) ID(s)

The IPT contains the details for a specific test (e.g., test execution procedures, dependencies on other tests, expected results, test date, actual/observed results, etc.). A template for the IPT will be provided by the Government to the Contractor upon contract award.

For the first submission of the RTM, all the IPT IDs will be empty. During IPC, the Contractor shall update the RTM with the IPT IDs for the requirements that are to be tested in IPC, as determined by the IPCDP (6.6.1.1.4 IPC Demonstration Plan (IPCDP)). Following IPC and for the remainder of the DREN4 Contract, the Contractor shall ensure the RTM is kept up-to-date anytime a change that affects the RTM occurs. For example, if the Government orders a CLIN post-IPC that has not yet been ordered, any related untested requirements in the RTM will need IPT(s) created and test(s) executed.

A template for the RTM will be provided to the Contractor following Contract award.

The Contractor shall review the RTM with the Government annually (6.4.1.9 Annual Planning and Design Review).

The Contractor shall submit the initial RTM to the Government no later than 60 days after contract award.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.6.1.1.2	RTM	Template provided by the Government following contract award	60 days after contract award		Standard Distribution (6.0.2)	One time, annually, and as required

6.6.1.1.3. IPC Implementation

The Government will utilize the IPC Plan, RTM, and other information to determine what will be ordered for IPC. Subsequently, the Government will place orders for the required CLINs.

Upon direction of the Contracting Officer, the Contractor shall follow the approved IPC Plan and implement the ordered CLINs. During implementation, the Contractor shall apply relevant security controls to all networks and systems in support of the RMF Assess and Authorization Process (6.6.1.2 Assess and Authorization Process). The initial set of firewall/ACL policies (6.3.4 Initial Boundary Protection Deployment) will be provided by the Government.

During execution of the IPC Plan, the Contractor shall utilize only Contractor-provided resources; no Government Furnished Equipment (GFE) shall be utilized. The Contractor shall complete the execution of the IPC Plan by completely implementing all required services from the ordered IPC CLINs no later than 150 days following direction by the Contracting Officer to begin.

6.6.1.1.4. IPC Demonstration Plan (IPCDP)

The IPCDP is the Contractor's detailed plan for conducting IPC Test and Demonstration. Using a combination of the RTM, IPC Plan, and the set of services the Government orders for IPC, the Contractor shall include in the IPCDP the following, at a minimum:

a) A list of RTM "Requirement IDs" to be tested during IPC Test and Demonstration

b) An IPT document for each test enumerated in the list

   1) The "Test Results" section of each IPT will be left empty for the IPCDP. These will be updated as a part of preparing the IPCDR (6.6.1.1.6 IPC Demonstration Report (IPCDR))

During the IPCDP development process, the Contractor shall submit each IPT individually. The Government will review and provide comments or acceptance of each IPT. At least 10 days before submitting the draft IPCDP, the Contractor shall submit all IPTs required for the IPCDP (i.e., part of IPC execution).

The Contractor shall submit the draft IPCDP to the Government no later than 120 days following submission of the final IPC Plan. The Government will then collaborate with the Contractor to finalize the IPCDP for the next 20 days. The Contractor shall then submit the final IPCDP to the Government.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.6.1.1.4	IPCDP	Contractor-Determined Format	Draft version 120 days after IPC Plan submission Final version 140 days after final IPC Plan submission		Standard Distribution (6.0.2)	One time

6.6.1.1.5. IPC Test and Demonstration

The IPC Test and Demonstration is the collection of test events from the IPCDP, with each event executed by following the test procedures in the associated IPT(s).

The Contractor shall begin execution of the test events upon direction from the Contracting Officer. Such direction shall not come before:

a) An IATT is issued

b) The Government has accepted the IPCDP

The Contractor shall complete the IPC Test and Demonstration no later than 53 days after commencement. The Government reserves the right to observe all test and demonstrations. The Contractor shall update each IPT with the results of each event.

6.6.1.1.6. IPC Demonstration Report (IPCDR)

The IPCDR is an update to the IPCDP. The Contractor shall begin with the IPCDP, ensure all IPTs are updated with results from IPC Test and Demonstration, and then submit as the IPCDR.

The Contractor shall submit the IPCDR, including copies of all updated IPTs for all tests and demonstrations, to the Government no later than seven days following completion of the IPC Test and Demonstration.

The Government will not disburse payment to the Contractor for services ordered for IPC until Government acceptance of the IPCDR. The Government does not intend to order and will not accept additional services (e.g., DREN Nodes) prior to acceptance of the IPCDR.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.6.1.1.6	IPCDR	Contractor-Determined Format	Seven days after completion of the IPC Test and Demonstration		Standard Distribution (6.0.2)	One time

6.6.1.2. Assess and Authorization Process

The Contractor shall upload all necessary RMF artifacts for the IATT (6.3.1.1 RMF IATT Package) to the Government no later than 220 days after contract award. The Government will then review the documentation and submit to the HPCMP AO in pursuit of an IATT.

The Contractor shall upload all necessary RMF artifacts for the ATO (6.3.1.2 RMF ATO Package) to the Government no later than 243 days after contract award. The Contractor shall perform an RMF self-assessment. The Contractor shall then support the Government execution of a SCA-V assessment. The Government will then pursue the ATO with the Approving Official (AO).

6.6.1.3. Comprehensive Implementation and Test Plan (CITP) Development

The CITP governs the actions associated with the provisioning, activation, and management of the remaining DREN Nodes during Phase II. During development of the CITP, the Contractor, in conjunction with the Government, shall determine optimal quantity, capacity, and placement of DCNs and DXPs, as well as the prioritization of the installation of all remaining DREN Nodes. The Contractor shall incorporate lessons learned during the IPC while developing the CITP.

The Contractor shall include in the CITP the following:

a) discussion, including challenges and risk mitigations, involving at least the following elements
    1) technical architecture
    2) subscriber transition
    3) interoperability
    4) security
b) discussion of the technical architecture throughout transition, including at least
    1) transition gateways
    2) how and when changes will be implemented
    3) special design considerations
c) DREN Node designs/architectures with specific details of each DREN Node type, functions, and services
d) DCN quantity, capacity, and placement recommendations (6.1.3.5 DCN Placement)
e) discussion to support the following capabilities during and subsequent to Transition
    1) ITS (6.1.2.11 Internet Transit Service (ITS) (Separately Orderable))
    2) peering (6.1.2.9.3 Peering)
        A) acquiring cross-connects at peering locations for connectivity to existing and new peers
        B) implementing peering with the same peers used on DREN III
        C) transport to commercial CSPs

3) interoperability with DREN III, including plans for

A) bridging existing layer 2 networks between DREN III and DREN4 at the transition gateways, with protections from loops

B) routing existing layer 3 networks between DREN III and DREN4, preserving proper separation between Collectives and Networks

f) projected timeline for installation of each DREN Node type, function, and service, including all activities and milestones for each

g) detailed actions and responsibilities for each step from initial identification of site, to installation and then Government acceptance

h) a detailed Subscriber cutover process, including the following

1) method for all required services being pre-provisioned and pre-configured, and activated upon connection by the Subscriber to the DREN Node without any further action by the DREN NOC

2) subscriber prerequisites identified, if any

3) coordination requirements for individual Subscribers as well as large groups of related Subscribers (same organization or program)

i) a detailed Subscriber cutover schedule, including the following

1) the defined frequency that scheduled updates will be published

2) procedures for handling schedule adjustments, delays, process failures, government-imposed delays, etc. with risk mitigations

j) naming convention, IP Addressing Plans, and DNS administration during transition (6.5.15 DNS Service)

The Contractor shall develop the CITP and submit the draft CITP no later than 200 days following contract award. The Government will then collaborate with the Contractor to finalize the CITP for the next 90 days. The Contractor shall then submit the final CITP.

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.6.1.3	CITP	Contractor-Determined Format	200 days after contract award		Standard Distribution (6.0.2)	One time, updated as required

6.6.2. Phase II

The transition of the remaining DREN III sites to DREN4 is collectively referred to as Phase II of Implementation and Transition. During Phase II, the Contractor shall:

a) Execute the CITP developed during Phase I

b) Cutover DREN III Subscribers to DREN4

The entrance criteria to Phase II is a successful completion of Phase I, acceptance of the final CITP, and Contracting Officer direction to proceed with execution of CITP.

The exit criteria for Phase II is a successful execution of the CITP, with all DREN III Subscribers identified by the Government cutover to DREN4. The Contractor shall complete Phase II no later than 365 days after the commencement of Phase II.

6.6.2.1. CITP Execution

Upon direction of the Contracting Officer, the Contractor shall begin executing in accordance with the approved final CITP. During this phase, the Government may issue one or more TSOs to initiate the transition of existing DREN III Subscribers or for new DREN services. The Government will issue a discrete TSO for each DREN Node (i.e., one site per TSO).

The Contractor shall install, document, and test all ordered DREN Nodes during Phase II in accordance with the PWS requirements.

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

6.6.2.2. Subscriber Cutover

The Contractor shall support the cutover of existing DREN III Subscribers to DREN4 with minimal interruption.

The majority of DREN Subscribers will utilize standardized SDP configurations and coordination to affect cutover. For these, the Contractor shall design and support a cutover such that all required services are pre-provisioned and pre-configured, and activated upon Subscriber connection to the DREN Node without any further action by the DREN NOC.

For the remainder of DREN Subscribers with more complex configurations, the Government will assist in the coordination, configuration, and activation of services with these Subscriber(s) to ensure a successful cutover.

6.6.3. 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 orders. The 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 DREN4 to replacement services are described in this subtask.

6.6.3.1. Planning and Engineering Support

The Contractor shall provide phase-out planning and engineering support that includes the following sub-elements:

6.6.3.1.1. 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 DREN4 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 shall 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 Contractor(s)

c) arrangements made with follow-on Contractor(s) for handling special features

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 Contractor(s) for purposes of transitioning to replacement services

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.6.3.1.1	Development of Contract and Network Phase-Out Transition Plan	Contractor-Determined Format	60 calendar days after award of follow-on DREN contract		Standard Distribution (6.0.2)	One time

6.6.3.1.2. Updating, Validating, and Transferring of Support Documentation

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

a) Inventory of service requirements for each DREN Node

b) Inventory of equipment at each DREN Node

c) Access link provider and other technical details

d) As-built diagrams

6.6.4. Network 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 the Government cancels service. The Contractor shall provide transition gateway support in accordance with the phase out transition plan.

7. PERFORMANCE STANDARDS

Task	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	Incentives (+/-)
6.0				

8. INCENTIVES

This PWS Section 6 includes negative incentives. Billing credits will be utilized for failure to meet performance standards only as identified in this PWS.

9. PLACE OF PERFORMANCE

This work shall be performed at the Contractor's facilities, Subscriber sites, Government sites and Peering locations as designated in the delivery orders.

10. PERIOD OF PERFORMANCE

The period of performance will be 120 months after contract award including a 48-month base period and three 24-month option periods. Up to an additional six-month period for unforeseen circumstances extends the period of performance to 126 months (as reference to FAR 52.217-8 is included in this contract).

11. DELIVERY SCHEDULE

PWS Task#	Deliverable Title	Format	Due Date		Distribution/Copies	Frequency and Remarks
6.0						

All deliverable materials and documents under this PWS shall be the property of the Government. All materials and documents provided online shall be available for download and unrestricted 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 DD-254, "Department Of Defense Contract Security Classification Specification" associated with this Contract.

12.1. Personnel Security

The Contractor shall conform to the provisions of DoDM 5200.02, DoD 5220.22-M, the Privacy Act of 1974, and related or referenced instructions.

The Contractor shall ensure all personnel that support DREN with administrative access have completed a favorably adjudicated Single Scope Background Investigation (SSBI) as a minimum investigation prior to being granted administrative privileges. The SSBI will be maintained current within 5 years and requests for Special Background Periodic Review (SBPR) will be initiated prior to the 5-year anniversary date of the previous SSBI or SBPR.

Pending completion of a SSBI and final adjudication for a security clearance, Contractor employees may be granted the necessary privileges to perform administrative duties as long as the following is met:

a) The request for an SSBI (via E-QIP or Word Fillable SF 86 and fingerprint cards) shall be submitted by the Contractor's Facility Security Officer (FSO) to the DCSA and the Joint Personnel Adjudication System (JPAS) reflects that the investigation is open and an Interim clearance has been granted.

The Contractor shall ensure that all personnel that have SDREN user access have at least a Secret Security Clearance.

The Contractor shall not claim lack of an appropriate investigation as a reason for noncompliance of investigation requirements for privileged access.

The Contractor shall submit to the Government completed DD 2875s for all personnel directly supporting the requirements specified in this Contract.

12.2. Email

The Contractor shall use Government provided dren.mil email accounts for the exchange of all data related to this Contract within 30 days of the Government acceptance of the IPC.

12.3. Visits

The Contractor shall:

a) comply with site security regulations including Government and non-Government. 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 or accessing Government facilities shall be subject to identification and badge requirements at those sites

b) submit requests for visit authorization in accordance with the policies and procedures of the location to be visited no later than one week prior to a non-emergency/urgent visit. Requests for visit authorization for Emergency or Urgent situations shall be in accordance with the policies and procedures of the location to be visited

12.4. Training and Certification

The Contractor shall:

a) comply with DoD Information Assurance (IA) Workforce Certification requirements. Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.239-7001 (Information Assurance Contractor Training and Certification) applies to this contract

b) ensure that its IA workforce members that support DREN have the baseline certifications corresponding to their IA functions, as defined in DoD Directive 8140.01, Cyberspace Workforce Management, and DoD 8570.01-M, Information Assurance Workforce Improvement Program at the start of an individual's performance on this contract

c) ensure that its IA workforce members that support DREN obtain all required Computing Environment (CE) certificates within six months after the start of an individual's performance on this contract. Functions spanning multiple levels require certification of the highest-level functions. Personnel performing functions in multiple categories or specialties shall hold certifications appropriate to the functions performed in each category or specialty

d) ensure that IAT Level I baseline certification is maintained for all IA workforce members supporting DREN with unsupervised privileged access

e) ensure that its IA workforce members that support DREN release their IA certification information to the DoD through the Defense Workforce Certification Application web site. The URL will be provided by the Government at contract award

f) ensure that all personnel supporting DREN with administrative access are properly trained and that they maintain technical proficiency for the operation and maintenance of systems and equipment that comprise DREN

g) ensure that all personnel with access to systems and networks that process Government information successfully complete initial cybersecurity and information assurance awareness orientation as a condition of access, and thereafter must complete annual cybersecurity and information assurance refresher awareness training (Cybersecurity and Information Assurance Awareness Orientation training URL will be provided by the Government at contract award). The Contractor shall maintain all cybersecurity and information assurance awareness orientation-training records and shall provide copies to the Government upon request

h) comply with DoD Directive 5205.02E, DoD Operations Security (OPSEC) Program. Failure to comply with the OPSEC directives shall be deemed adequate cause for the removal of a Contractor's employee from performance on this contract and could be considered for appropriate legal action. The Contractor shall ensure all personnel performing work under this contract complete Level I OPSEC training within 30 days of start of an individual's performance on this contract and annually thereafter (Level I OPSEC training URL will be provided by the Government at contract award). The Contractor shall maintain all OPSEC training records and shall provide copies to the Government upon request

i) ensure that all personnel performing work under this Contract with privileged/administrative access create a user account and profile in the Army Training and Certification Tracking System (ATCTS) websiteat "https://atc.us.army.mil", in the unit container managed by the Government

j) ensure that all personnel performing work under this Contract with privileged/administrative access provide to the Government:

1) certificates of successful completion of IA training

2) signed Acceptable Use Policies (AUP)

3) signed User Agreements

4) signed Privileged User Agreements

5) appointment Memorandums

6) applicable baseline and computing environment certifications

7) continuing professional education credits as required by DoD 8570.01-M for upload into the ATCTS

k) ensure that all personnel with access to ACAS successfully complete Government on-line DISA related ACAS Training

l) ensure that all personnel with view only access to the section of the ePolicy Orchestrator (ePO) application that controls the implementation of HBSS on Contractor deployed servers and workstations successfully complete Government on-line HBSS 201 Reviewer Training

m) ensure that all personnel with administrative access to the section of the ePolicy Orchestrator (ePO) application that controls the implementation of HBSS on Contractor deployed servers and workstations successfully complete Government on-line HBSS 301 Administrator Training

12.5. Common Access Card (CAC)

Contractor personnel directly supporting the requirements specified in this Contract shall obtain a DoD CAC.

The Contractor's FSO shall ensure that all Contractor personnel that directly support the requirements specified in this Contract PWS acquire and maintain a DoD CAC.

The Government will only sponsor Contractor personnel that are directly supporting the requirements specified in this Contract.

CACs expires when Contractor personnel are no longer supporting the requirements specified in this Contract, three years from the issuance date or the expiration of this Contract, whichever occurs first.

The Contractor shall immediately return individual CACs obtained for use under this contract to the Government whenever Contractor personnel are no longer supporting this Contract or upon the expiration of this Contract.

The Contractor is responsible for safeguarding all CACs issued for supporting the requirements specified in this Contract and shall report all lost or stolen CACs to the Government immediately.

The Contractor shall acquire and utilize a DoD approved middleware and software solution to read DoD issued CACs.

12.6. 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 that physical security is applied in accordance with DoDI 8500.01, Cybersecurity; DoD 5200.08-R, Physical Security Program; and DoD 5220.22-M, NISPOM

12.7. Facility Clearance

The Contractor shall acquire a final Secret Facility Clearance (FCL) from the DCSA Facility Clearance Branch (FCB) at the DREN Helpdesk location(s) to support the requirements to establish and maintain connectivity to SDREN as specified in this Contract, no later than 90 days after Government acceptance of the DREN IPC.

12.8. Protection of Sensitive and Classified Data

The Contractor shall:

a) Comply with all requirements specified within all volumes of DoD Manual 5200.01.

b) Ensure compliance with all DoD Personnel Security Requirements for access to Controlled, Unclassified Information (CUI) and Secret Information.

c) Not install or connect IT applications or systems not under the governance of a DoD Component Cybersecurity Program to DREN.

d) ensure that any sensitive information, including, but not limited to, CUI, PII [Personally Identifiable Information] and FOUO [For Official Use Only], proprietary, and Law Enforcement Sensitive information residing on Mobile Computing Devices (MCD) or other external media, is protected in accordance with current Data at Rest guidelines and requirements. MCDs include, but are not limited to, laptop, netbook, notebook, or tablet computers, and Portable Electronic Devices. External media include optical disk media such as Compact Discs (CDs), Digital Video Discs (DVDs), and other portable digital storage devices

e) utilize, if necessary, only approved USB drives (also referred to as flash or thumb drives) to transport any sensitive data

12.9. Media Sanitization and Disposal

There are two primary types of media in common use:

a) Hard Copy. Hard copy media are physical representations of information, most often associated with paper printouts. However, printer and facsimile ribbons, drums, and platens are all examples of hard copy media. The supplies associated with producing paper printouts are often the most

uncontrolled. Hard copy materials containing sensitive data that leave an organization without effective sanitization expose a significant vulnerability to "dumpster divers" and overcurious employees, risking unwanted information disclosures.

b) Electronic (i.e., "soft copy"). Electronic media are devices containing bits and bytes such as hard drives, RAM [random access memory], ROM [read-only memory], CD, DVD, flash memory, memory devices, phones, MCD, networking devices, office equipment, and many other types.

Clear, Purge, and Physical Destruction are actions that can be taken to sanitize media. The categories of sanitization are defined as follows:

a) Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

b) Purge applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

c) Physical Destruction renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

12.9.1. Unclassified Media Sanitization

If a media used to store Unclassified DREN information is planned for reuse by the Contractor to support DREN either the Clear or Purge technique shall be used.

All other planned reuse shall use the Purge technique.

If media is not intended for reuse either within or outside the Contractor's organization due to damage or other reasons it shall be physically destroyed.

Media used by the Contractor to store DREN information shall not be returned as part of a Return Merchandise Authorization (RMA).

12.9.2. Classified Media Sanitization

If media used to store classified information is planned for reuse by the Contractor, the Purge technique shall be used and the media shall only be reused at the same classification level it for which it was originally utilized.

If media used by the Contractor to store classified information is not intended for reuse at the same classification level within Contractor's organization due to damage or other reasons it shall be physically destroyed.

Media used by the Contractor to store classified information shall not be returned as part of a RMA.

Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. A certification of media disposition will be an electronic record of the action taken. The person performing the sanitization shall record the following details required for the certificate as the media is sanitized.

Contractor Media Sanitization Records shall be provided to the Government upon the completion of each media sanitization performed. These records shall be maintained by the Contractor for three years.

Media utilized by the Contractor to store DREN or classified data shall not be returned to the Government unless requested by the Government.

When fully completed, the certificate shall record at least the following details:

- Manufacturer
- Model
- Serial Number
- Organizationally Assigned Media or Property Number (if applicable)
- Media Type (i.e., magnetic, flash memory, hybrid, etc.)
- Media Source (i.e., user or computer the media came from)
- Pre-Sanitization Confidentiality Categorization (optional)
- Sanitization Description (i.e., Clear, Purge, Destroy)
- Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.)
- Tool Used (including version)
- Verification Method (i.e., full, quick sampling, etc.)
- Post-Sanitization Confidentiality Categorization (optional)
- Post-Sanitization Destination (if known)
- Name of Person for Both Sanitization and Verification:

Failure to comply with Media Sanitization requirements specified in this contract will result in a security incident due to a spillage.

APPENDIX A. ACRONYMS

[NIST] Special Publication (SP) 51
Access Control List (ACL) 26
Acquisition Engineering (AE) 10
Adjusted Network Availability (ANA) 90
Advanced Research Projects Agency Network (ARPANET) 10
Aggregate Unavailability (AU) 91
Any Source Multicast (ASM) 21
Application Programming Interfaces (APIs) 14
Army Training and Certification Tracking System website (ATCTS) 122
Assured Compliance Assessment Solution (ACAS) 54
Assured Forwarding (AF) 22
Asynchronous Transfer Mode (ATM) 9
Authorization to Operate (ATO) 53
Authorizing Official (AO) 53
autonomous systems (ASs) 23
bandwidth delay product (BDP) 18
Best Current Practices (BCPs) 17
Bootstrap Router (BSR) 21
Border Gateway Protocol (BGP) 21
British Thermal Unit (BTU) 48
Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 51
Cloud Service Provider (CSP) 10
Commercial Solutions for Classified (CSfC) 72
Committee on National Security Systems Instruction (CNSSI) 51
Committee on National Security Systems Policy (CNSSP) 51
Common Access Card (CAC) 85
Communication Security (COMSEC) 63
Community of Interest (COI) 11
Compact Discs (CDs) 123
Comprehensive Implementation and Transition Plan (CITP) 10
Concept of Operations (CONOPS) 53
Configuration Control Board (CCB) 61
Connection Approval Process (CAP) 64
Contract Line Item Number (CLIN) 11
Contracting Officer (KO) 15
Contracting Officer representative (COR) 8
Controlled, Unclassified Information (CUI) 123
Cyber Protection Condition (CPCON) 62
Cybersecurity Services Provider's (CSSP) 54
Defense Counterintelligence and Security Agency (DCSA) 64
Defense Information Systems Agency (DISA) 9
Defense Research and Engineering Network (DREN) 8
Defense Research and Engineering Network 4 (DREN4) 8

Denial of Service (DoS) 62
Department of Defense (DoD) 8
Department of Defense Activity Address Code (DODAAC) 8
Differential Services (DiffServ) 22
DiffServ Code Point (DSCP) 22
Digital Video Discs (DVDs) 123
Distributed Denial of Service (DDoS) 26
DoD Instruction (DoDI) 51
Domain Name System (DNS) 27
DREN Active Measurement Program (DAMP) 43
DREN Core Node (DCN) 13
DREN eXchange Point (DXP) 13
DREN Joint Sensor (DJS) 43
Equal-Cost Multi-Path (ECMP) 18
Ethernet Virtual Private Network (EVPN) 18
Expedited Forwarding (EF) 22
Extended DMZ (ED) 23
External Gateway Protocol (EGP) 17
Global Positioning System (GPS) 72
Graphical User Interface (GUI) 37
High Performance Computing (HPC) 8
High Performance Computing Modernization Program (HPCMP) 8
Indefinite Delivery/Indefinite Quantity (ID/IQ) 9
Individual Performance Test (IPT) 112
Information Operations Condition (INFOCON) 52
Information Security Continuous Monitoring (ISCM) 59
Information System Security Manager (ISSM) 53
Information System Security Officers (ISSOs) 53
Initial Performance Capability (IPC) 10
Interim Authorization to Test (IATT) 53
Interior Gateway Protocol (IGP) 17
Intermediate System – Intermediate System (IS-IS) 23
International Telecommunications Union (ITU) 29
Internet Assigned Numbers Authority (IANA) 27
Internet Control Message Protocol (ICMP) 21
Internet Engineering Task Force (IETF) 17
Internet eXchange Points (IXPs) 14
Internet Group Management Protocol (IGMP) 21
Internet Protocol (IP) 9
Internet Service Providers (ISPs) 17
Internet Transit Service (ITS) 14
Intrusion Detection Systems (IDSs) 62
IP Security (IPsec) 9
IP version 4 (IPv4) 20
IP version 6 (IPv6) 20
IPC Demonstration Plan (IPCDP) 109

IPC Demonstration Report (IPCDR) 109
Joint Force Headquarters-DoD Information Networks (JFHQ-DODIN) 62
Managed Trusted Internet Protocol Service (MTIPS) 17
Maximum Transmission Unit (MTU) 21
Media Access Control (MAC) 39
Media Access Control Security (MACsec) 12
Mobile Computing Devices (MCD) 123
Modeling and Simulation (M&S) 10
Monthly Recurring Charge (MRC) 78
Multicast Listener Discovery (MLD) 21
Multicast Source Discovery Protocol (MSDP) 21
Multi-Exit-Discriminators (MEDs) 23
Multi-Mode (MM) 48
MultiProtocol Border Gateway Protocol (MBGP) 23
Multi-Protocol Label Switching (MPLS) 9
National Information Assurance Partnership (NIAP) 15
National Institute of Standards and Technology (NIST) 18
Navy/Marine Corps Internet (NMCI) 22
Network Control (NC) 19
Network Function Virtualization(NFV) 12
Network Junction Points (NJPs) 13
Network Operations Center (NOC) 9
NFV Infrastructure (NFVI) 45
Non-Classified IP Router Network (NIPRNet) 15
North America Network Operator's Group (NANOG) 17
Office of the Designated Approving Authority (ODAA) 64
Office of the Designated Approving Authority (ODAA) Business Management System (OBMS) 64
Open Shortest Path First (OSPF) 23
Performance Work Statement (PWS) 1
Per-Hop Behaviors (PHB) 22
Plain Old Telephone Service (POTS) 81
Priority-based Flow Control (PFC) 40
Program Management Review (PMR) 68
Protocol Independent Multicast-Sparse-Mode (PIM-SM) 21
Provider Backbone Bridging (PBB) 40
Quality of Service (QOS) 19
Rack Units (U) 47
Request for Comments (RFC) 21
Requirements Traceability Matrix (RTM) 109
Research and Development (R&D) 10
Research and Education (R&E) 9
Risk Management Framework (RMF) 12
Round Trip Time (RTT) 18
Routing Arbiter DataBase (RADB) 26
Science and Technology (S&T) 10
SDP Lite (SDP-L) 15

Security Content Automation Protocol (SCAP) 54
Security Control Assessor-Validator (SCA-V) 60
Security Gateway (SG) 12
Security Requirements Guides (SRGs) 55
Security Technical Implementation Guide (STIG) 54
Service Delivery Point (SDP) 13
Shortest Path Bridging (SPB) 18
Simple Network Management Protocol (SNMP) 36
Single-Mode (SM) 48
Software Defined Networking (SDN) 12
Source Specific Multicast (SSM) 21
Standard Operating Procedures (SOPs) 53
Technical Interchange Meeting (TIM) 67
Telecommunications Service Order (TSO) 75
Telecommunications Service Request (TSR) 80
Test and Evaluation (T&E) 10
Total Network Availability Possible (TNAP) 91
Transmission Control Protocol (TCP) 14
TRansparent Interconnection of Lots of Links (TRILL) 18
Tunnel Termination Point (TTP) 48
Virtual Local Area Networks (VLANs) 12
Wide Area Network (WAN) 9