Volume I, Appendix A – Table of Contents

This page intentionally left blank.

A. Wide Area Connectivity Plan

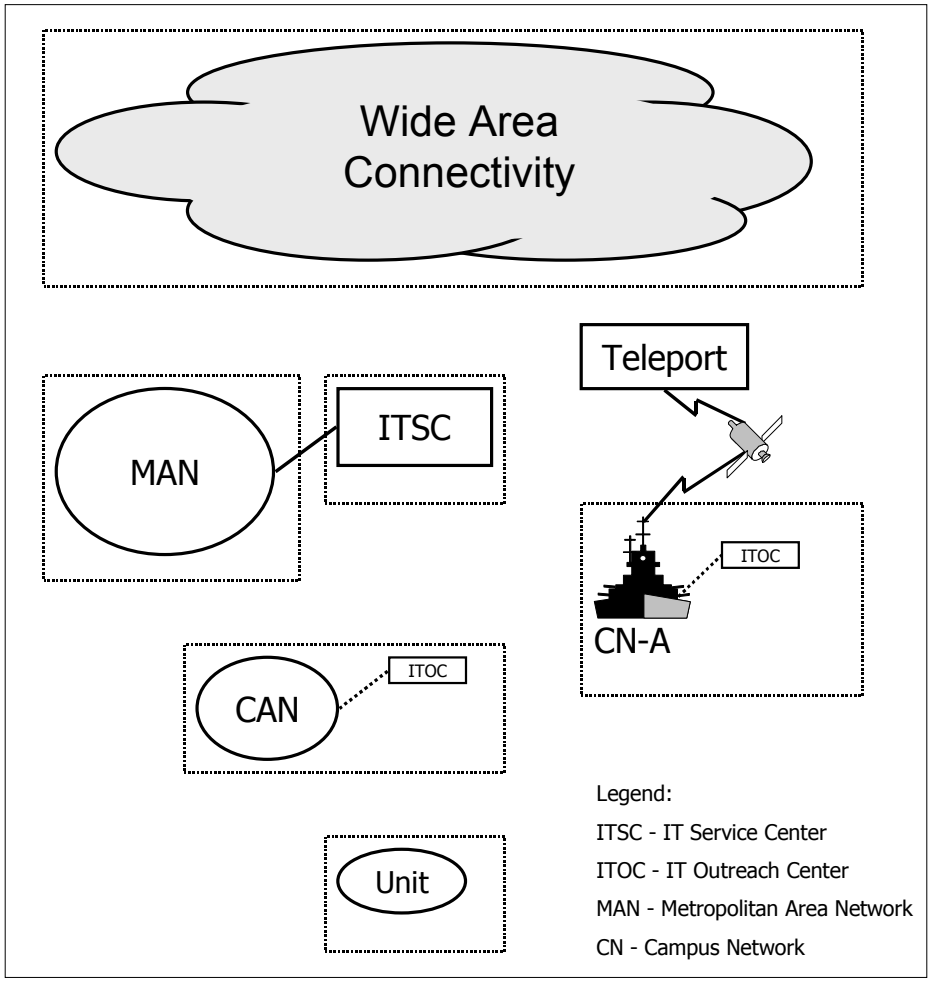

Figure A-1. High Level Components of the TI Artchitecture

A.1 Introduction

Purpose of the Wide Area Connectivity (WAC) Plan. The principal requirement for the WAC Plan is to outline the strategy and steps to plan and establish a wide area network (WAN) that interconnects all of the DON Metropolitan Area Networks (MANs). Figure A-1 shows the relationship of the Wide Area Network (WAN) to the other components of the Information Technology Infrastructure (ITI) Architecture.

The detail, considerations, and steps in this WAC Plan are consistent with the importance placed on this function by the Navy and Marine Corps. The WAC represents the essential interconnectivity between the organizational elements of the DON enterprise network. Its uniquely complex and inter-related planning requirements necessitate a carefully orchestrated, integrated DON approach.

This WAC Plan provides scope and definition, approach, strategy, and implementation milestones to be used by TI planners to design and implement a DON WAN. This plan will be consistent,

complementary, and interoperable with the overall DON enterprise network as defined by the accompanying planning templates contained in this enterprise network architecture.

This WAC approach is supported by industry best practices and is essential for Naval conformance with the Clinger-Cohen Act of 1996 and the Office of Management and Budget memorandum 97-16.

A.2 Operating Environment

The WAC Plan must address the connectivity of all Navy and Marine Corps organizations, including joint services and supporting contractors, in the following environments:

- **MAN and Outlying Campuses.** As discussed in the network architecture Section 3.1, the MANs provide efficient and effective connectivity to the Naval concentration areas. The purpose of the WAC is to interconnect these MANs
- **CONUS and OCONUS.** Naval concentration areas include both continental U.S. (CONUS) and outside continental U.S. (OCONUS) areas. OCONUS examples include Naples, Bahrain, and Yokosuka. This WAN document initially places emphasis on but does not limit itself to the CONUS areas.
- **Ashore and Afloat.** The terrestrial WANs provide the trunk technology and switching to interconnect the Metropolitan Area Networks (MANs), including afloat units at piers.

For underway and deployed forces, the architecture guidance for the global connectivity provided through satellite communications (SATCOM) and Line of Sight (LOS) radio links is provided separately.

A.3 Definition of Connectivity and Services

A.3.1 Wide Area Connectivity

Definition. WAC provides connectivity that interconnects widely-separated components of the Naval enterprise by interconnecting the Naval MANs. The WAN complements the other network connectivity components and provides end-to-end connectivity across the Navy and Marine Corps units.

Points of Connectivity. The WAN includes long-haul circuits and the ATM switches. The WAN provides connectivity between the MANs (and in some instances, directly to some outlying campuses/bases). As shown in Figure A-1, the WAN includes delivery through shore-based, satellite, at-sea, and other mobile platforms. It addresses connection to the external networks – Defense Information System Network (DISN), Non-secure IP Router Network (NIPRnet), Secure IP Router Network (SIPRnet), Defense Research Engineering Network (DREN), Defense Switched Network (DSN), and the Internet.

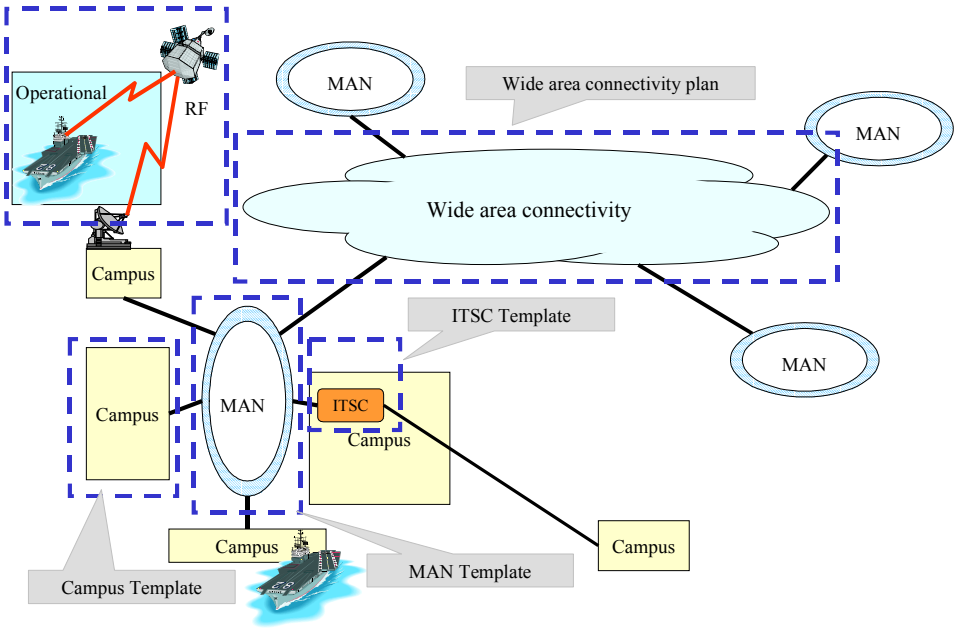

Figure A-1. Wide Area Connectivity Components and Demarcations

Demarcations. The major demarcations for the WAN are the locations of the Metropolitan Area Networks (MANs) and the Information Technology Service Centers (ITSCs). These MANs and ITSCs represent the geographic locations and levels of the DON organization at which most technology infrastructure services planning, implementation, and operation are performed. The MANs and ITSCs figure strongly in determining the DON WAN service functionality and performance.

In specific instances, the ITSCs are the fleet teleports that directly link the WAN to the fleet using a variety of interworking components including satellite and line-of-sight RF links to extend the enterprise network to overseas, deployed, and embarked units.

A.3.2 Wide Area Services

The WAN infrastructure relies upon Asynchronous Transfer Mode (ATM) as its principal technology. ATM enables the consolidation of voice, video, and data onto a single network and offers the advantages of speed, economy, and interoperability for the entire spectrum of networking applications.

Physical Layer – The WAN must support the interconnection of the ATM services in the MAN and campus networks in a way that preserves an end-to-end ATM cell delivery and signaling service. It is expected that the physical layer will be provided by Synchronous Optical Network (SONET) transmission systems for the carrier ATM networks that interconnect the Naval MANs.

Network Management – The MANs and subordinate networks will be managed by the ITSCs. The WAC provider will manage the backbone connectivity, but must also provide enough visibility of the WAC to the ITSCs for DON network managers to eliminate ambiguities and/or isolate failures.

The functions of network management are grouped in three categories: those performed by the WAN service provider, those provided by DON enterprise network management centers, and those performed by the ITSCs.

- **Service Provider Services** - These functions are listed by the name of their top level of granularity. Selected guidance is included for certain functions. The WAN functions provided by the service provider include the following:
  - Network monitoring - The WAC provider must provide sufficient visibility of SNMP monitoring information to allow DON ITSC managers to correctly isolate faults to the correct provider.
  - Configuration management
  - Routing management - The WAC provider must minimize routing hops in the virtual circuits that interconnect the MAN routers and switches.
  - Trouble response
  - Performance management - The WAC provider must provide a stated bandwidth and assurance that this can be easily scaled to meet requirements.
  - Fault management - The WAC Plan must explain how trouble ticket support will be performed. The respective responsibilities of the WAC trouble desk versus the ITSC trouble desk require definition. These should be consistent across the enterprise.
  - Security management
  - Network metrics
- **DON Enterprise Management Services** - The functions performed by the DON enterprise management centers are those of an administrative service nature and include ATM and IP address management. The DON Network Information Center (NIC) administrates the ATM addressing plan and the end system addresses. The NIC is also the DON single point of contact for both IP and Network Service Access Point (NSAP) registration. The DON Addressing Plan is provided in Chapter 4. The NIC services are described in the ITSC template (Appendix D).
- **ITSC Services** - The balance of the required services are performed by the ITSCs. These ITSC functions are delineated in Appendix D and Chapter 4.

A.4 Acquisition Strategy

Subscription Based on Functionality. The overall DON strategy for obtaining enterprise backbone services is one of subscription – coordinated, carefully determined, and consistently implemented subscription of services. Multiple DON organizations and multiple commercial service providers may team to acquire the aggregation of WAN services that provide the complete, robust, and efficient interconnectivity required by all Navy and Marine Corps organizations. These services extend to units operating in CONUS and OCONUS regions and to deployable units operating at sea, in remote sites, and pier-side.

In the case of CONUS regions, each region provides connectivity to all other regions either directly or through neighboring regions. The collection of regions, the services they provide, and the connectivity between them constitute the DON enterprise network. It is through implementation agreements and the design factors and architecture guidance in this document that the DON regions successfully share responsibility of a well-designed and managed DON enterprise network.

Service Level Agreement. The subscription of services will be based upon very specific service level agreements that include functional specifications as well as performance specifications. This WAC Plan will help provide guidance to participating DON organizations to adequately define

these specifications. This will ensure that the required functionality, performance, and business case analysis guidance is specifically stipulated in resulting Request for Proposals and in subsequent contracts that define these services.

Competitive Strategy. Determining functionality, performance, and cost (business case analysis) factors of the backbone services requires multi-disciplinary skills for planning and implementation. The responsibilities for implementing the WAC plan include development of the specification and design, execution of the acquisition and funding, and operation and maintenance. The WAC Plan will provide a context for evaluating and selecting the factors that pertain to these three responsibilities.

A.5 Functional and Performance Specifications

In most cases, the WAN is described not in terms of design guidance, as is the case of MAN and campus templates, but in terms of service levels or outcomes. In other words, the government will specify the required services but not the specific implementation architecture. Exceptions to this will occur only when specific technologies are required for functionality or interoperability. For example, the architecture will not specify SONET but will require ATM. The service provider will be allowed to use the architecture and technology solutions that best achieve the specified services and provide the best business practices cost. The specifications are stated in a form that provides an empirical level of expectation and description of the services to be provided.

The services provided by the WAN are in five categories: security, functionality, interoperability, performance, and cost. The level of service, and in some cases, the specific technologies required, are described for each. These specifications are provided as a guide; actual requirements may warrant adjustment of these values but this should be based on solid documentation.

- **Security -** Few security mechanisms are allocated to the wide area connectivity. For the protection of classified information, cryptographic equipment is required. For the security of the infrastructure, the solution is to provide redundancy in the network components. Redundancy should be used when available. The use of Simple Network Management Protocol (SNMP) and remote monitoring of critical networking components such as switches, multiplexers, and routers should be emphasized and control of these is warranted whenever possible. This architecture details the appropriate mechanisms that must be supported.
  - Hardened
    - Level of service: must provide a sufficient level of protection for denial of service and intrusion detection.
    - Technology: N/A
  - Survivability (specifically relating to security) (see also Performance)
    - Level of service: intrusion detection, denial of service, and vulnerability to service attacks. The WAC provider is responsible for these only as they relate to the WAC-provided service. They will normally consist of data link layer encryption services (e.g., Fastlane).
    - Technology: N/A

- **Functionality -** The capabilities required of the network infrastructure that are necessary to effectively and efficiently support the operational mission and requirements must be clearly defined.
  - ATM
    - Level of service: support voice, video, and data.
    - Technology: end-to-end switched virtual circuit (SVC) and permanent virtual path (PVP).
  - MAN connectivity
    - Level of service: each MAN is provided access to two geographically-separated WAN switches. This is directly related to Availability (Ao) and Survivability.
    - Technology: N/A
  - Switch functionality
    - Level of service: must support constant bit rate (CBR) QoS.
    - Technology: non-blocking and provide separate queuing for different Quality of Service (QoS) classes. WAN switches will support at least 2048 switched and/or permanent virtual circuits (PVCs) per interface.
  - Availability
    - Level of service: accessible to all MANs and outlying bases. (See also Network Availability for additional Availability requirements.)
    - Technology: N/A
- **Interoperability -** The components of the network infrastructure must interconnect and efficiently and effectively communicate signaling and other information transfer data.
  - Service Delivery Points (SDPs)
    - Level of service: must support the full suite of ITSG-cited ATM protocols and addressing schemas. The WAC SDP must be able to provide the required support of DON IP requirements as well as the cited Interior Gateway Protocols, Exterior Gateway Protocols, and firewalls.
    - Technology: N/A
- **Performance -** The WAN service must be sufficiently qualified to meet the following information transfer requirements to support the Naval mission:
  - Bandwidth
    - Level of service: minimum of OC-3.
    - Technology: redundant dual-homed.
  - Delay
    - Level of service: maximum end-to-end delay for CBR service connection should be less than 200 us/hop for processing and queuing time plus the necessary propagation delay (5 us/km). The maximum end-to-end cell delay variation should be less than 1 ms.

  - Technology: N/A
- Latency
  - Level of service: if switched point-to-point SVC or SVP is supported, the maximum latency in completing a call setup must be less than 100 ms/hop plus propagation delays.
  - Technology: N/A
- Network availability
  - Three principles of high availability are established: (1) eliminating single points of failure, (2) reliable crossover, and (3) prompt notification of failures as they occur. All three must be accounted for in the performance metrics.
  - Network monitoring is an issue that requires visibility. A problem in monitoring network availability is determining the failure point when something breaks. The normal situation is for the commercial vendor and base telecommunications to each deny responsibility. Through the ITSC, the capability should exist to immediately sort out the failure point and to call the correct repairman. One means is SNMP visibility of the vendor's network—having access in the ITSC to the real-time availability data that the vendor system monitors are indicating. Having this access should be part of the WAN service provider specification.
  - Level of service: 99.99 percent.
  - Technology: no switch or physical circuit is a single point of failure.
- Survivability (specifically relating to performance - see also Security)
  - Level of service: vulnerability to forces of nature and human action, including enemy action (i.e. backhoe, power loss, terrorist strike).
  - Technology: no switch or physical circuit is a single point of failure. It is strongly recommended that the service provider’s assumptions for survivability be carefully investigated and validated.
- Quality of Service
  - Level of service: ability to support a number of service classes based on the traffic type, each with an associated QoS parameter.
  - Technology: N/A

- **Cost -** Implementation cost is an important category for judging value and must be done in the context of the level of service.

A.6 Potential WAN Service Providers

The DON CIO policy for subscription of WAN services is based on a competitive strategy. The functionality and performance of the service must support that required by the individual MANs and be provided at a competitive price. When DISA can provide the same or equal service at the same or less cost, they will be the preferred service provider. When DISA is not competitive with alternative service providers, subscription will be obtained elsewhere based on best value.

A.7 Potential WAN Service Providers

Three service providers are suggested for consideration. They each have specific strengths and weaknesses that must be weighed in a WAN decision. The WAC Plan could use the services of one or all three, or there may be other more acceptable approaches such as a DON-administered contract to a commercial provider.

DISA

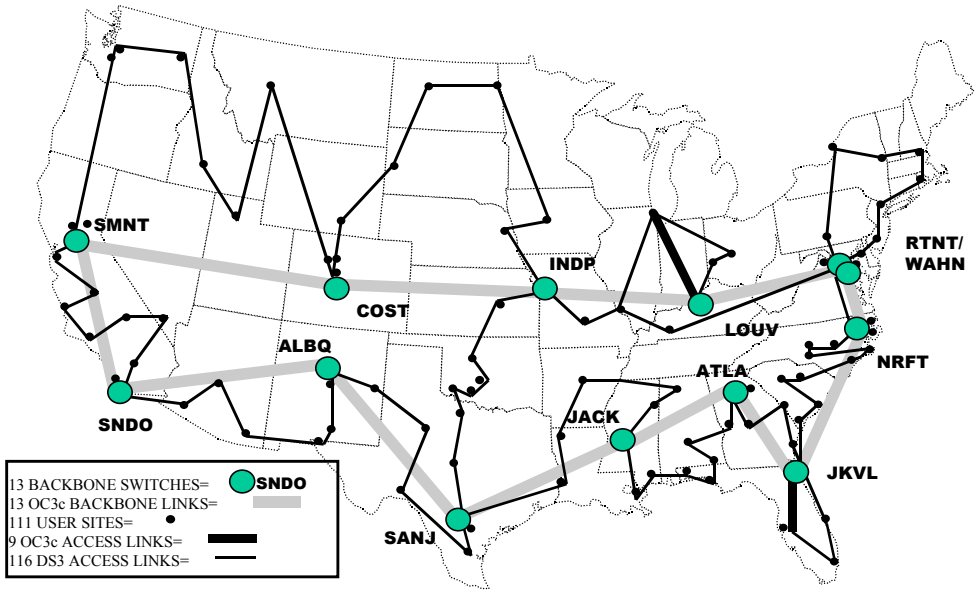

Figure A-1. DISA Wide Area Network Connectivity

The top level view of the Defense Information Systems Network (DISN) in Figure A-1 shows the CONUS ATM service provided by DISA. DISN services in the OCONUS environment represent a near global coverage for Navy and Marine afloat, combat ground, and ashore operating units. In July 1998, 50 ATM nodes were available globally for DoD units. By October 1998, the number of nodes was estimated at 125. The projection for December 2001 is 200.

SmartLink

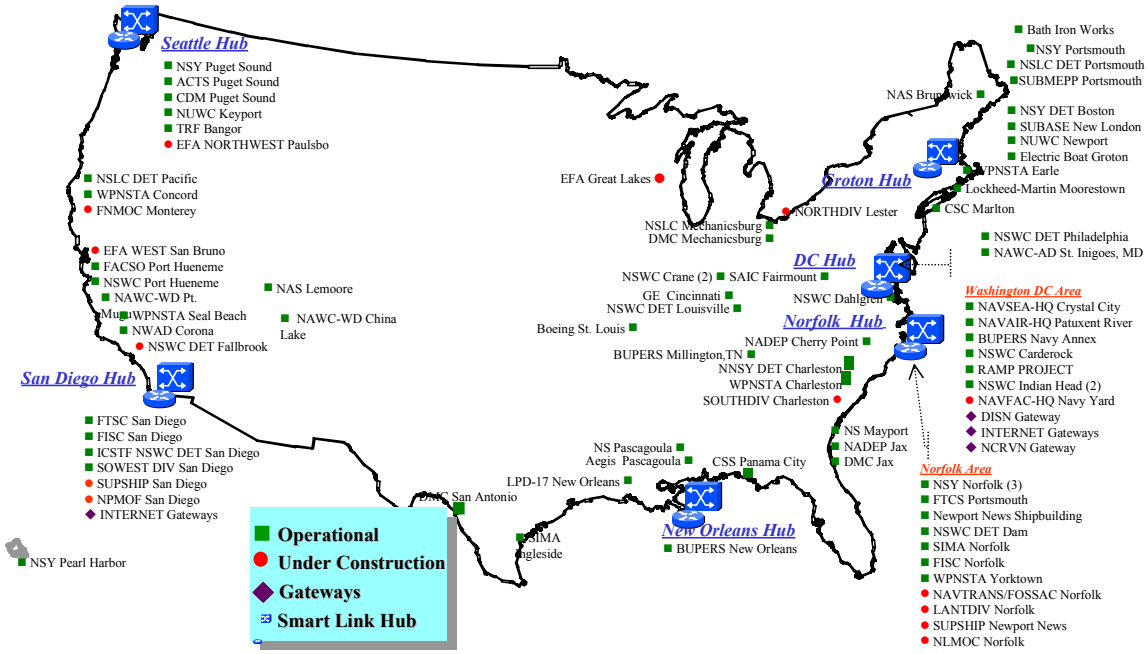

Figure A-2. SmartLink Wide Area Network

The top level view of the SmartLink Backbone Plan depicted in Figure A-2 shows SmartLink's long-haul SONET circuits, ATM switches, and wide area supporting services. This backbone plan is aligned with the fleet concentration areas described in Chapter 2-4. Accordingly, the plan provides an ATM switch at each of the identified concentration areas. SmartLink provides connectivity between the regions (and in some instances, directly to some outlying campuses/bases).

DREN

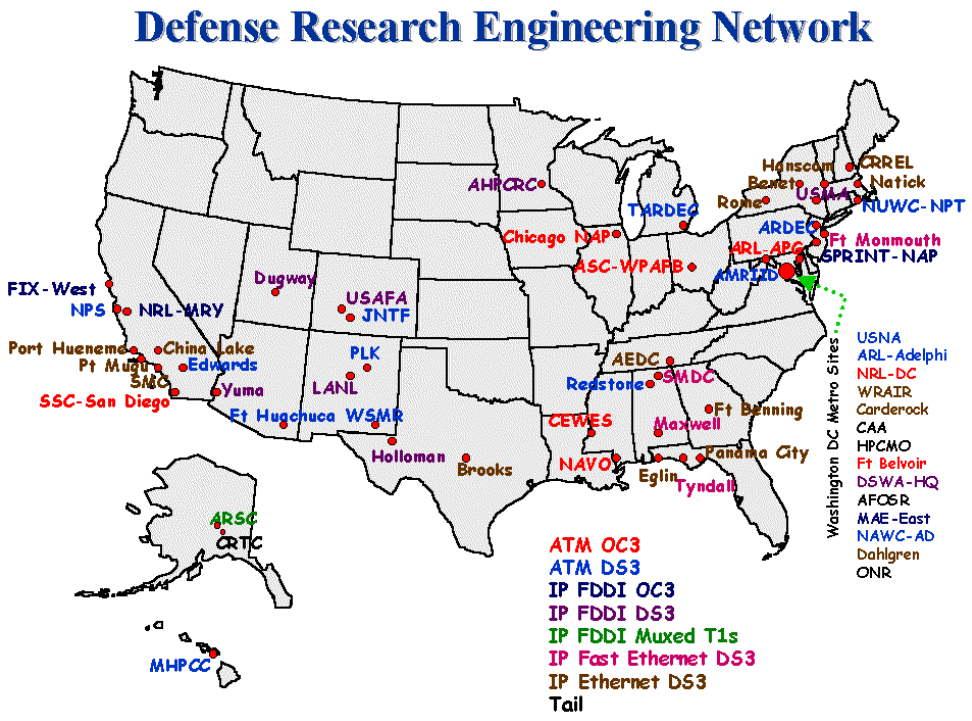

Figure A-3. DREN Wide Area Network

Defense Research Engineering Network (DREN) is a DoD WAN used to link DoD scientists and engineers. The DREN project provides wide-area ATM networking services at bandwidths that are commensurate with DON user communication requirements. ATM connectivity currently includes over 20 CONUS locations.

A.8 Evaluating WAN Service Providers

The WAN services source determination will be made by a DON Integrated Product Team (IPT) comprised of representative (Navy and Marine Corps, tactical and non-tactical, afloat and ashore) operational and functional experts.

The determination will be made based on a balanced scorecard approach using as a basis the characteristics defined in the functional and performance specifications in section A.5. Addressing the proposals of each competing WAN service provider will be performed in accordance with the criteria in Figure A-1.

Network Characteristic	Raw Score	Weighting (.xx)	Adjusted Score
Network Security	X	.30	X
Functionality	X	.25	X
Interoperability	X	.25	X
Performance	X	.20	X
Total	—	1.0	X
Total Merit / Cost	—	—	X/$YY

Figure A-1. Service Provider Evaluation

Four of the five characteristics will be scored based on a numerical rating system (1-10). The supporting subsets of each characteristic will be evaluated and aggregated to determine the value of the characteristic.

Also, each characteristic will have a weight factor based on its judged importance to the overall Naval mission. The total of these individual weighting factor will be 1.0. Recommended weighting factors are provided.

The numerical value for each characteristic is multiplied by its weight factor and the total of the five adjusted scores equals the relative merit for the source provider.

Cost will be viewed as a separate variable. The relative merit will be expressed in terms of a ratio of total merit to cost (e.g, X / $ YY).

A.9 Plan of Action for Selecting WAN Service Provider(s)

The DON CIO Board of Representatives will charter an IPT or task a standing IPT to select a service provider(s) of DON's Wide Area Network services. This team will include individuals with appropriate acquisition experience.

The IPT will evaluate alternative sources to meet the DON enterprise WAN requirements as defined by DON mission requirements. The solution will be consistent with this DON ITI Architecture document and the DON Information Technology Standards Guidance.

The WAN services to be provided must consider wide area connectivity today, what is required, and consider the best way to resolve the service gap. The resulting strategy must identify specific:

- Sites within MANs and those outside

- Sites for which service points of presence exist and those outlying sites that have significant investment, implementation, or provider issues (tail circuits, OCONUS remote sites, and technology change over)

The IPT will use the outline of the balanced scorecard to develop a data sheet for the purpose of going to DISA, SmartLink, and DREN (and potentially others) to ask for a prospectus of WAN services provided via Request for Proposals (RFPs). The RFP shall place emphasis on obtaining complete data so that meaningful comparisons can be made.

The IPT will complete an analysis of the alternative providers and present a recommendation in writing to the Board of Representatives. Included in the presentation will be a recommendation for the administration and funding of the WAN.