

Volume I, Appendix D - Table of Contents

D. ITSC Design Template.....	D-1
D.1 Purpose.....	D-1
D.2 ITSC Drivers.....	D-2
D.3 ITSC Customers.....	D-2
D.4 Elements/Features/Specifications.....	D-3
D.4.1 ITSC Connectivity to WAN, MAN, and CAN.....	D-4
D.4.2 ITSC Security Architecture.....	D-5
D.4.3 ITSC Levels of Connectivity Service.....	D-6
D.4.4 Description of ITSC Services Provided.....	D-7
D.5 Hierarchical Service Structure ITSC and ITOC.....	D-20
D.6 ITSC Infrastructure Physical Attributes.....	D-21
D.7 Metrics.....	D-21

This page intentionally left blank.

D.ITSC Design Template

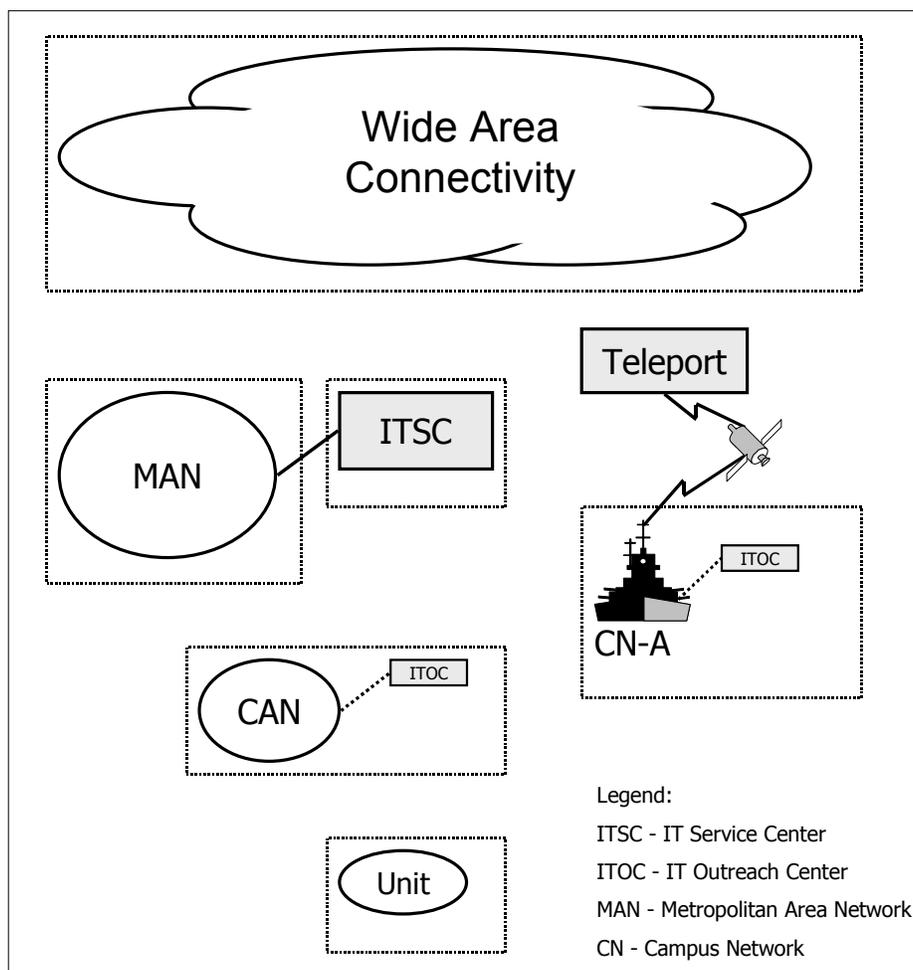


Figure D-1. High Level Components of the TI Architecture

D.1 Purpose

Figure D-1 depicts the relationship of the Information Technology Service Center (ITSC) to the other components of the Information Technology Infrastructure (ITI) Architecture. The ITSCs are operated by the Navy and Marine Corps and provide essential network services.

The collection of ITSCs in the DON forms a cohesive, interconnected, integrated, and interoperable network management community that is dedicated to providing infrastructure support for Navy and Marine organizations. The ITSCs, like the network they support, have the capability to manage voice, video, and data transmission. The ITSC-supported ITI promotes economies and efficiencies by reducing and consolidating redundant services and performing them in such a way that they earn "provider of choice" status among the Navy and Marine Corps user organizations.

In order to support the DON enterprise network, there is a need for cohesive strategy, consistent planning and implementation, and resultant maximum services interoperability and performance. This architecture must provide sufficient guidance for separate and geographically distant regions to independently implement a Navy- and Marine Corps-determined number of ITSCs that mutually support a DON enterprise network management capability.

This ITSC template establishes a consistent means to address the delivery of these network services, identifies appropriate instances for specific service solutions, and provides a detailed list of implementation considerations. This template is intended for use by ITI planners and implementers and should guide all future network management implementations at all Navy and Marine Corps ITSCs.

D.2 ITSC Drivers

The DON network infrastructure and services must support the diverse and demanding mission requirements of the Navy and Marine Corps. The ITSC architecture solution must satisfactorily meet the following:

- The network infrastructure, and by extension, the ITSC management structure must be supported as a single integrated system consistent with the stated goals of network centric warfare.
- The DON ITSC template must specifically address fleet and mobility issues.
- The location of ITSCs will be determined by criteria that includes the following factors:
 - ◆ geographic distance and distribution
 - ◆ user population density
 - ◆ information technology expertise currently demonstrated
 - ◆ alignment with the operational chain of command
 - ◆ military service mission
- The DON must achieve efficiency through ITSC consolidation but not at the expense of reliability and quality service.
- There must be accountability for ITSC performance in any DON ITSC management solution and customers must be assured of quality service, responsiveness, and best value.
- The ISO model for network management is applicable to organizing the ITSC management functions and will serve as a framework for addressing ITSC-specific responsibilities.

D.3 ITSC Customers

ITSCs must address the network services of all DON customers residing in their areas of responsibility. Generically, the ITSCs must support the following categories of customers:

- Commands not connected via an ITSC-serviced regional MAN with organic servers
- Commands not connected via an ITSC-serviced regional MAN and with no organic servers
- Deployed and underway units

- Commands connected via an ITSC-serviced regional MAN (e.g Tidewater MAN connecting all Campus Area Networks (CANs) in the Tidewater region)
- Information producer commands
- Small units or users on travel
- Interface to the DISN Regional Control Centers (RCCs) and Global Control Center (GCC) under the DII control concept for all DISN access issues within a region

D.4 Elements/Features/Specifications

Figure D-1 provides the outline to address the elements, features, and specifications of the ITSC. The ITSC is described first in terms of its relative position in the WAN, MAN, and CAN topologies and the associated requirements for survivability and security. A concept of service levels provides a means to identify and address the diversity of DON organizational connectivity and service requirements. A description of the services to be provided by the ITSC forms the main body of this template. The relationship of the ITSC to the Information Technology Outreach Center (ITOC) is described. The ITSC physical architecture references the requirements of the ITSC physical infrastructure as provided in the DON Information Technology Standards Guidance (ITSG). Finally, for eventual ITSC implementation, metrics are considered to be essential to gain the necessary acceptance of the major organizations of the Navy and Marine Corps.

1. ITSC Connectivity Relationships to WAN, MAN and CAN		
2. Concept of ITSC Levels of Connectivity Service		
3. Description of ITSC Services Provided		
Network Operations <ul style="list-style-type: none"> • Help Desk • Fault Management • Security Management • Performance Management • Accounting Management 	Network Administration <ul style="list-style-type: none"> • Capacity Planning • Security Planning • Domain Name System • Dynamic Host Configuration Protocol • Directory • Public Key Infrastructure • Configuration Management 	ITSC Supported User Services <ul style="list-style-type: none"> • Network Time Protocol • Email • News/Network News Transfer Protocol • Web • File Transfer Protocol • Remote Access • Multimedia
4. Hierarchical Service Structure of ITSC and ITOC		
5. ITSC Infrastructure Physical Attributes		
5. ITSC Metrics		

Figure D-1. ITSC Connectivity and Services Outline

D.4.1 ITSC Connectivity to WAN, MAN, and CAN

The elements and features of the ITSC architecture can best be explained in a layered approach. The graphic depicted in Figure D-1 shows the physical connectivity of some of the network components.

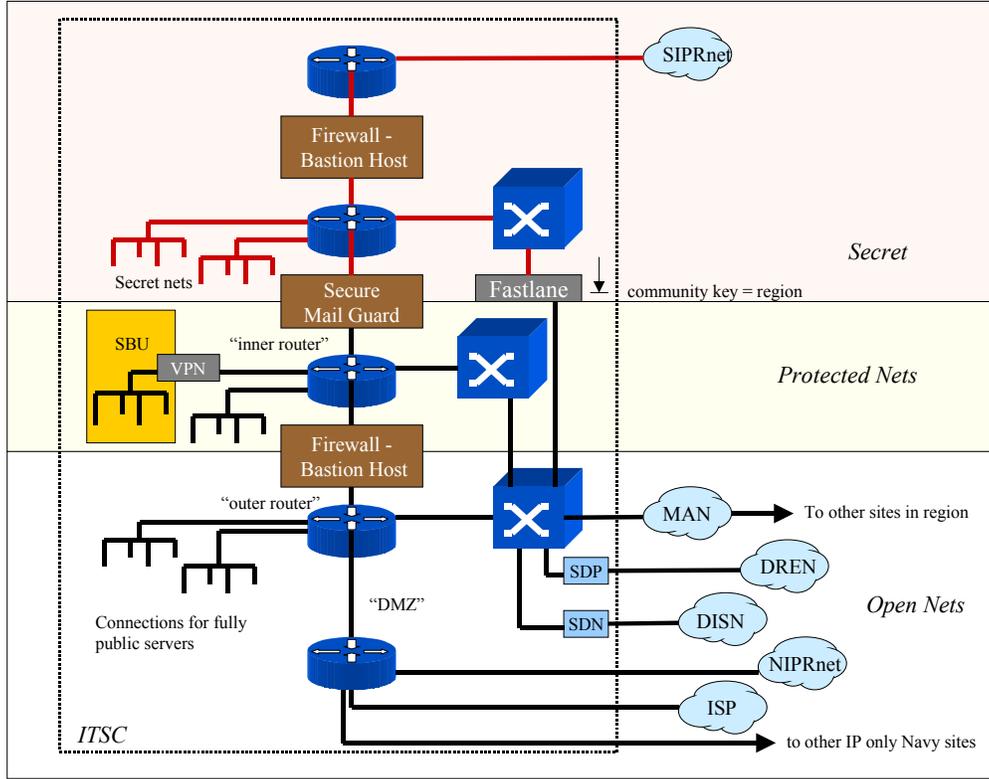


Figure D-1. ITSC Physical Connectivity Layout

The "open networks" shown in the bottom part of Figure D-1 run across the MAN and to the wide area in the clear. They are primarily used for the Demilitarized Zone (DMZ) and peering type functions and for connecting public services.

For unclassified network services, there are two separate logical networks – the Open Nets (outer unprotected connectivity) and the Protected Net (inside the firewall). The campuses will need to access one or the other, or both. The logical separation of these networks is not reflected in this diagram but is accomplished through ATM virtual circuits. For sensitive but unclassified (SBU) network services, VPN technology will be used to encrypt information as it is carried over the networks that are external to the base.

Additional architecture detail can be represented by the logical connectivity that is supported by the ATM Virtual Circuits (VCs) and Virtual Paths (VPs) that ride on top of the depicted physical layout. The VCs and VPs are not shown in the above diagram.

The typical path for a campus to get Internet connectivity is to go through Fastlane encryption. To get SBU network connectivity, the typical path is over the MAN to the ITSC and through Fastlane. In both cases, it is transported through the firewall and onto the NIPRNET and other Internet Service Providers (ISPs) using the IP protocol.

Campuses that have back-door connections to ISPs will not be allowed to connect (via the Fastlanes) inside the firewall. They will connect to the “outer net.”

D.4.2 ITSC Security Architecture

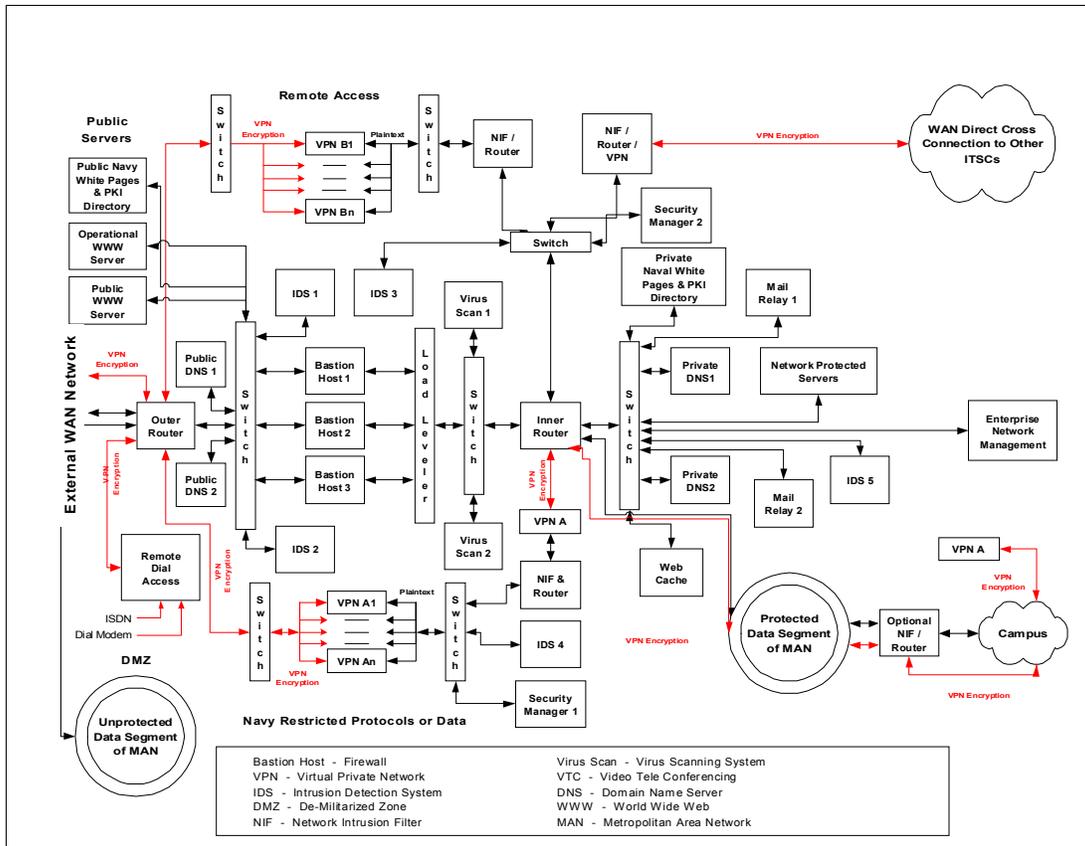


Figure D-1 ITSC Security Template

The template depicted in Figure D-1 describes the various functional components of the ITSC security architecture and how they interconnect. This template should be used for the design of ITSCs.

The template reflects the standard Naval firewall design, which includes the outer router, bastion hosts, inner router, public and private DNS servers, virus scanners, mail relays, and intrusion detection systems. The template also includes an IP “Load Leveler” which performs load balancing across the three bastion host firewalls in order to provide improved scalability.

Most servers are connected behind the firewall in order to protect them from unauthorized external access. The exceptions are the public servers that are connected to the outer router. These servers would be blocked from external access if they were connected inside the firewall. The representative servers shown here are the web servers and a directory (Navy white pages).

For access to the protected services from outside the firewall (remote access), there is a “firewall bypass” using Virtual Private Network (VPN) technology. User who gain access will need to use VPN client software and certificate based authorization. This access from the unprotected side is supported by strong authentication and a fully encrypted path.

For application specific protection where “dangerous” protocols need to pass through the firewall or remote networks need virtual connectivity behind the firewall, there is additional VPN functionality to meet those requirements. In such cases, the data is broken out into the clear to perform intrusion detection and filtering before re-encryption for distribution in the region.

The MAN is illustrated as having both a “protected data segment” and an “unprotected data segment”. This possibility of multiple segments illustrates that a single physical MAN infrastructure will have a number of separate logical networks to support its multiple requirements. Campus networks will be connected to a MAN on the logical segment that matches its connectivity requirements. In order to connect to the protected data segment, campus networks must completely eliminate all other external connections (back doors). The unprotected data segment is primarily for external connectivity and for peering on the DMZ.

Campuses should still employ intrusion filters and possibly VPN technology even when connected to the protected data segment of the MAN. This added protection supports the DoD “Defense in Depth” approach.

The depicted web cache not only provides added security through its proxy functionality, but also serves a very important function of reducing the consumed bandwidth and the number of connections across the firewall. All web queries to the outside are forced to go through the web cache.

D.4.3 ITSC Levels of Connectivity Service

Levels of service in a MAN or region must address two aspects. First, the level of service for the most demanding customer establishes the highest level of service that must be provided in a MAN or region. To some extent, this level influences the level of service for other users. For example, many applications share the same connectivity, but only a few require the high levels of availability that necessitate 24-hour monitoring and backup connectivity. However, when those services are in place for the demanding users, others may benefit at little or no additional cost. Conversely, premium service requires premium levels of effort and it is obviously not economical to provide that level of service to everyone. The maintenance response for specific applications and associated servers can and should be tuned. It is inappropriate to provide 24-hour application maintenance support for administrative applications that are used only during daytime working hours.

The following generic levels of service and their definitions are established for the DON by this architecture document. Importantly, levels should not be determined by the rank or grade of the commander or official in charge but should be based primarily on the service appropriate to the characteristics of the information required to support the organizational mission.

The following service levels will be consistently applied, as appropriate, for planning and implementation of all connectivity and network services provided by the ITSC.

- Level 1 (High) – Includes operational commands (and certain admiral/general level staffs). Characterized by intense high volume and real-time response network traffic. These commands require 24 x 7 support for all or some network devices.
- Level 2 (Medium) – Includes organizations, staffs, and/or commands that experience interim periods of intense high volume traffic but require a moderate bandwidth and service response. Hours of operation to be supported are normally daytime working hours.

- Level 3 (Low) – Administrative commands (and certain operational and staff commands) that have a moderate to low requirement for network bandwidth and services and require normal response times for performing business-related activities.

D.4.4 Description of ITSC Services Provided

D.4.4.1 Network Operations Center

The Network Operations Center (NOC) services as outlined in Figure D-1 include the network management link to the customer that allows the customer to provide notification of network problems and to receive feedback regarding resolution. These NOC services also include the monitoring services (fault management, security management, and performance management) that enable network managers to monitor the network performance and take corrective actions to improve the network performance in response to both performance degradation and failures. These NOC services support network communications that are mission critical and require timely resolution.

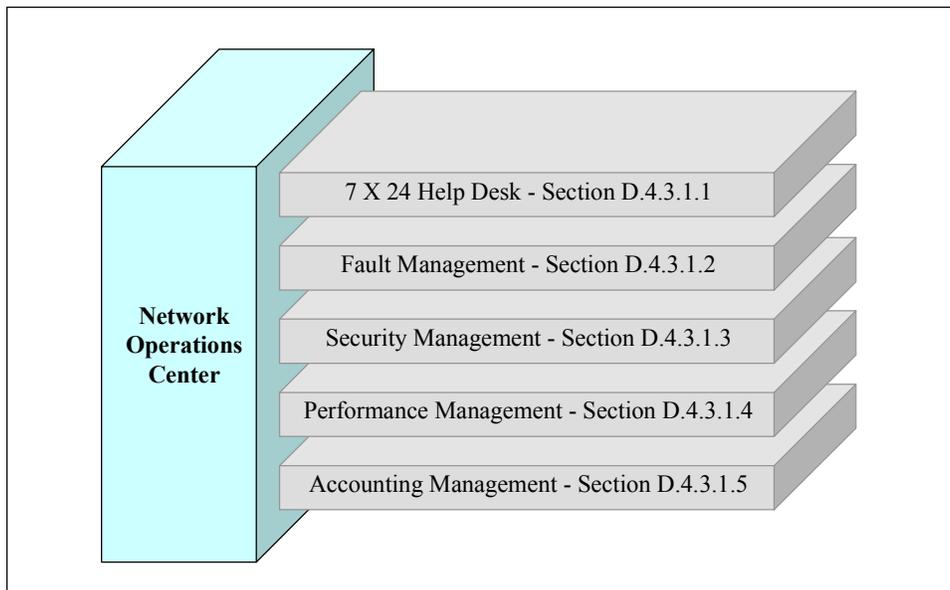


Figure D-1. Network Operations Center Services

D.4.4.1.1 7 X 24 Help Desk

Description: The ITSC Help Desk includes the services associated with end user support. It is responsible for providing multiple resources to solve network computing issues to the client's satisfaction. The Help Desk will be an integrated service provider and will be a single point of contact for all customers who need assistance. By interoperating with all other ITSCs, it will be able to provide tracking, escalation, information sharing, and contingency back up. Specific Help Desk service guidance includes the following:

- Trouble ticket origination and tracking
- Pass off and escalation scheme
- Tracking system database structure

- Recommended fields (schema) for regional trouble tracking databases

Guidance: At a minimum, the ITSC Help Desk services will include the following:

Trouble Ticketing Origination and Tracking.

1. Tracking tools must be integrated with standard fault isolation and reporting tools to enable automatic ticket generation.
2. The Help Desk application must be World Wide Web (WWW)-capable so users can submit and query statuses.

Pass Off and Escalation Scheme

1. There will be a minimum of 3 tiers of support, with tier 1 being the lowest and tier 3 being the highest.
2. All trouble calls are initiated as tier 1 by the ITSC and escalated by the ITSC.
3. Trouble tickets raised to tier 2 and 3 will be fielded on a priority basis with on-call support available outside of normal business hours.
4. Escalation of calls to higher tiers will be performed automatically by mission criticality and case-by-case.
5. Inter-regional pass offs are conducted as follows:
 - ♦ The activity receiving the report will record receipt of the ticket.
 - ♦ The affected region will be notified by the tracking system and must acknowledge receipt.
6. Completed action will be reported to the originating activity.
7. Interaction with cognizant vendors to resolve problems will be conducted by a designated single ITSC entity.

Tracking System Database Structure

1. The Help Desk tracking system will use a single relational database management system.
 - ♦ Initially, each region will have a single RDBMS that is consistent across the enterprise.
 - ♦ Regional systems will migrate to a single enterprise RDBMS.
 - ♦ RDBMS “core” schema must be coordinated across the enterprise.
 - ♦ Core schema must also accommodate regional/local requirements.
 - ♦ This tracking system will also support ITOC requirements.
2. The Help Desk schema will:
 - ♦ standardize the transfer of tickets and retrieval of information among the ITSCs, and
 - ♦ be flexible in its design to allow customization for special local needs without impacting the base application.
3. The system will use a Help Desk software tool to generate and display graphs summarizing relevant performance metrics.
4. Current unresolved issues between the trouble ticketing system and Casualty Reports and Unit Reports should be addressed to minimize duplication of reporting requirements.

5. Base level ITOCs must have access to the tracking system.

Recommended Fields (Schema) for Regional Trouble Tracking Databases

- Help Desk category (what the trouble is)
- Caller identification (who called the trouble in)
- User of the affected system (if other than caller)
- Affected system (software or hardware)
- Affected system component (software or hardware)
- Description of problem (use technical terminology)
- Criticality of work affected (at a minimum, mission critical, mission non-critical)
- Internally-generated tasks (not a trouble call but a task to be done)
 - ♦ Generated adds/changes (e.g., computer move)
 - ♦ Internally-generated tasks from network or configuration management systems
- Location of action (building, ship etc.)
- Location amplification (department, room, deck, etc.)
- History of escalation (what level, when, etc.)
- Special handling (special requirements)
- Action completed (use technical terminology)
- Inventory affected (equipment changed or software modified for forwarding to configuration management)
- Follow-on response warranted (yes or no)

D.4.4.1.2 Fault Management

Description: Fault management includes the management tools that support the availability of user systems by providing the ability to perform fault detection, isolation, and correction. This is the means of promptly notifying the Help Desk of failed equipment, which is an essential component of high availability networking. Fault management includes:

- Monitoring and collection of statistics on traffic conditions and use so potential faults can be forecasted and avoided. This is done by the network manager, who polls various agents for these statistics and assembles the resultant data for viewing (and logging for trend analysis).
- Alarms that warn of threshold conditions on the network that may cause failures. The alarm thresholds are set with SNMP sets and are triggered by SNMP traps.
- Alarms that warn of performance degradation on servers, switches (networks and phone), routers, and area network links. Also, alarms that warn of resource use problems such as low disk space on a server.

Fault management (the first of three ITSC network monitoring functions) allows the NOC to centrally view fault indicators on managed devices remotely and to make corrective adjustments. It requires network management agents in deployed network equipment (e.g. network management agents in routers, hubs, switches, UPSs, as well as end systems and software

processes) that the manager interacts with to collect, fuse, filter, and display data. Such interaction requires devices that support enabling standards (e.g., SNMP 2-3 (Simple Network Management Protocol), RMON-II (Remote Monitoring Protocol), MIB-II (Management Information Base)).

Guidance: At a minimum, ITSC fault management services will:

- Provide concise and in-depth views of network connections in a graphical format to provide the ability to evaluate network performance, preempt network disruption, and anticipate network growth or realignment.
- Monitor network capacity and use to project future expansion needs. As growth occurs (e.g., new workstations, printers, routers, web servers, and other devices), these tools provide an indication of corresponding required network enhancements.
- Identify network components that exceed set thresholds. Data trends are generated to provide analysis of network condition and developing trends.
- Consolidate network topology into simplified maps to enable generation of multi-level reports that enable robust analysis for optimizing performance at each level. Complex networks are easily viewed to recognize potential bottlenecks and balance network resources for optimal efficiency.
- Forward, by agent, the specific network events from appropriate collection sites to ITSC to ensure that events get appropriate attention. Event notification is by color-coded Graphical User Interface (GUI). Events include:
 - ◆ Equipment failure
 - ◆ Communications loss
 - ◆ Overloaded components
 - ◆ Improperly configured components
- Enable monitoring and notification of local specific events necessary to support specific environments.
- Provide the capability to isolate monitoring of carriers' frame relay, the local telephone companies' circuit, the customers' equipment, and users' applications. One means of accomplishing this is for the local telephone company to export the appropriate SNMP data to the NOC's network manager.
- Enable access to all management information at a single console. All pertinent data will reside on a single ITSC repository.
- Resolve problems and perform actions automatically whether the network is up (in-band) or down (out-of-band).

D.4.4.1.3 Security Management

Description: Security management includes assessment of the managed infrastructure's security posture. It also includes resistance and detection of intrusions and other information protection infractions. Security management will:

- Monitor normal performance of network components and attached end systems. The first indication of a security violation is often abnormal performance.

- Positively control firewall configurations.
- Operate intrusion detection software (most implementations examine packets at firewalls screening for villains).
- Document intrusions in an evidentiary manner suitable for supporting possible law enforcement action.

Security management (the second of three ITSC network monitoring functions) allows the NOC to centrally view security indicators on managed devices remotely and to make corrective adjustments. It requires network management agents in deployed network equipment (e.g., network management agents in routers, hubs, switches, UPSs, as well as end systems and software processes) that the manager interacts with to collect, fuse, filter, and display data. Such interaction requires devices that support enabling standards (e.g., SNMP 2-3, RMON-II, MIB-II).

Guidance: At a minimum, ITSC Security Management services will:

- Monitor existing systems on a 7 X 24 basis to detect insecurities such as spoofing or break-in attempts.
- Monitor network traffic to detect denial of service attacks such as Syn-floods or Smurf attacks.
- Monitor critical processes to ensure that they are not replaced by eavesdropping versions of the processes.
- Maintain intrusion-resistant integrity on network equipment (e.g., proper password control for routers).
- Maintain end system security resistance commensurate with the end system's use. An example is a password sweep to detect easily-breakable passwords.

D.4.4.1.4 Performance Management

Description: Performance management enables informed network performance decisions based on three major categories of performance data: network or site location, physical access circuits, and virtual circuits services. Also included is demand management, which addresses mission and other contingencies that arise that impact normal IT operations and decision-making. For instance, normal IT decisions might be overridden in the event of a resource crisis or other non-IT priority. Specifically, performance management includes:

- Guidance for establishing a plan of monitoring multiple protocol layers and alerts to network operations when performance deviates from normal.
- Corrective actions based on early warning signs to keep network operation at peak efficiency.
- Selective viewing of WAN events by customer network, site, or priority level to allow continuous assessment of performance.

Performance management (the third of three ITSC network monitoring functions) allows the NOC to centrally view performance indicators on managed devices remotely and to make corrective adjustments. It requires network management agents in deployed network equipment (e.g., network management agents in routers, hubs, switches, UPSs, as well as end systems and software processes) that the manager interacts with to collect, fuse, filter, and display data. Such interaction requires devices that support enabling standards (e.g., SNMP 2-3, RMON-II, MIB-II).

Guidance: At a minimum, ITSC performance management services will:

- Report on health of the network on a continuous basis.
- Monitor and tune existing systems on a 7 X 24 basis to ensure optimum use of hardware resources and ensure that agreed performance and throughput levels are maintained. These service levels can be monitored by the ITSC on an exception basis.
- Use performance management to respond to short-term needs and use capacity planning to respond to long-term needs using modeling tools.
- Monitor the network for potential or impending bottlenecks and congestion. Examples of indicators include the following:
 - ♦ Contention-based Ethernet – loading beyond 30 percent
 - ♦ FDDI – loading approaching 96 percent
 - ♦ Telephony – congestion in voice switch resulting in inordinate busy signals
 - ♦ ATM – to be determined
- Report on the server load balancing for servers such as Domain Name System, Dynamic Host Configuration Protocol, web, and Network Time Protocol using diagnostic tools.
- Use performance management data to update capacity planning models on an annual (minimum) or as-needed basis.
- Provide for contingency plans to react appropriately to arising Performance Management information and to allow stabilization of the networks in crisis conditions.

D.4.4.1.5 Accounting Management

Description: Fee-for-service is an important element of network management. Instances in which agencies other than DON obtain network services from organizations within DON must be accounted for in a satisfactory billing arrangement.

Guidance: This will be a topic for future guidance.

D.4.4.2 Network Administration

Network administration, shown in Figure D-1, includes a number of services that support planning for future requirements and administration of network-related functions of a less time-critical nature (e.g., Domain Name Service). These functions are associated with the traditional Network Information Center (NIC).

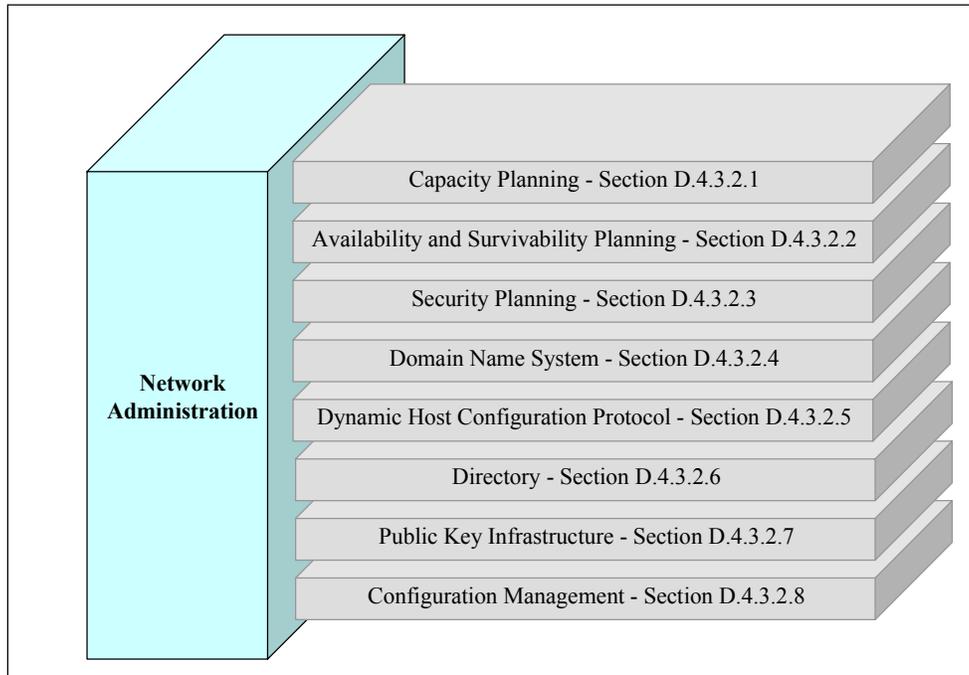


Figure D-1. Network Administration Services

D.4.4.2.1 Capacity Planning

Description: Capacity Planning, which is defined as using modeling to plan changes to the infrastructure, estimates the volume and variety of the workload. It supports analysis of results to ensure that service levels can be maintained and that no major bottlenecks occur.

Guidance: At a minimum, ITSC Capacity Planning services will:

- Use workload forecasts to produce estimates of IT infrastructure requirements to meet service objectives.
- Maintain the following items in a logical information repository:
 - ◆ topology data for the environment,
 - ◆ inventory of equipment,
 - ◆ user workload profiles, and
 - ◆ baseline models representing current resource use.
- Generate forecasting scenarios (simulations) from the repository to plan for meeting service level objectives.
- Use capacity planning methodology to forecast the performance of an active or a proposed system.
- Create a “baseline” of the existing environment that reflects the performance of the infrastructure. The model must be broken into sufficient detail to permit development of resource profiles for each system contained within the model.
- Use capacity planning information to:
 - ◆ estimate future workload growth/change,
 - ◆ forecast the likely use of hardware resources as workload varies,
 - ◆ forecast expected performance and throughput levels for that system, and
 - ◆ project workload requirements and translate them into demands for IT resources.
- Accept information for modeling software from standard ITSC network management tools.

D.4.4.2.2 Availability and Survivability Planning

Description: Availability and Survivability include planning for alternate/redundant connectivity, distribution of routing and switching components, and network monitoring.

Guidance: At a minimum, ITSC availability and survivability planning services will:

- Estimate mission critical systems and plan redundant connectivity (i.e., without single points of failure) to support them.
- Examine existing infrastructure for creeping requirements. Networks tend to attract mission-critical requirements over time that did not exist on the original installation.
- Ensure that installation of networking equipment eliminates or minimizes single points and common cause failures. Examples include:
 - ◆ provide separate UPSs for duplicate equipment (e.g. routers),
 - ◆ ensure that alternate connectivity enters premises through different cable trenches than the primary connectivity, and
 - ◆ places routers in different rooms/buildings so that a fire will not disable both

- Ensure that networking equipment has fault monitoring agents so that failures can be monitored by the NOC. Planners/implementers must ensure that mission critical end systems and applications have SNMP agents for monitoring purposes.
- Plan for appropriate backup power and power distribution for extended electrical outages. For example, when diesel generators are used as a second tier behind uninterruptable power supplies, the generator power must be distributed to routers, hubs, and switches that may be fed by several different power panels.
- Arrange backup peering arrangements between ITSC NOCs so that the failure of an ITSC can be compensated for by neighboring NOCs.
- Plan exercises to test the system.

D.4.4.2.3 Security Planning

Description: Security Planning (or Information Protection) includes planning for redundant and complementary security mechanisms that provide information protection consistent with the mission.

Guidance: At a minimum, ITSC information protection management services will:

- Provide guidance for application developers that incorporate security features in a system early in the planning cycle. Ensure that application developers understand utility-of-object level security that uses the Public Key Infrastructure (PKI) support structure.
- Examine current and planned applications for unintended security leaks. For example, does an application inadvertently make network vulnerabilities visible to an eavesdropper?
- Plan exercises to test information protection ability. Such exercises should test the attrition capability of multiple layers of the defense, not just the ability to withstand attacks on one feature.

D.4.4.2.4 Domain Name System (DNS)

Description: DNS is the service that translates domain names to IP addresses and vice versa. A domain name is a mechanism to give unique names to network devices so that users need not remember their numerical IP addresses. The service is implemented as a hierarchical distributed database and is accessed using a client/server model. The server component of DNS is the subject of this discussion.

Guidance: The DNS services description, as provided in Chapter 4, is fully applicable for ITSC implementation.

D.4.4.2.5 Dynamic Host Configuration Protocol (DHCP)

Description: DHCP supports a number of features that are useful to customers of the network. They include:

- Automatic assignment of IP addresses and configuration data such as netmasks and Domain Name System (DNS) servers.
- Immediate assignment of addresses that are actually used, which results in economic use of IP addresses because unused addresses are reclaimed for reuse.

- Easy system administration because of automation and the ability to administer these details from the server rather than the client.

DHCP is not intended to support mobile users, but it is valuable in supporting dynamic laptop network attachment at remote locations.

Guidance: At a minimum, ITSC DHCP services will encourage use of DHCP to provide some elements of mobility within the campus.

While DHCP is not intended to support mobile users, it is also valuable in supporting dynamic laptop network attachment at remote locations.

D.4.4.2.6 Directory

Description: Directory Services provides a phone book “white pages” function and offers a repository for other information such as phone numbers (office, fax, pager, mobile, and Secure Telephone Unit (STU)), e-mail addresses, and mailing addresses. Additionally, the service is expected to be used for other information about individuals, including passwords, digital certificates, and emergency contact information.

Newer client applications are becoming “directory aware” and use standard protocols to locate information. The dependence of these client applications on directories is increasing its importance in the technology infrastructure.

Guidance: The directory services description as provided in Chapter 4 is fully applicable for ITSC implementation.

D.4.4.2.7 Public Key Infrastructure (PKI) Administration.

Description: Public key availability is critical to several security applications, including secure e-mail, secure SNMP management, and secure web service. ITSCs will maintain a public key distributed database that is authentic and complete and will include the public keys of all Naval personnel.

Guidance: At a minimum, ITSC PKI services will support the following.

- Commands will generate public and private keys at their level.
- The private key is given to an individual (e.g., by floppy disk, smart card) or to a command custodian.
- The public key must be transmitted, along with the personal data, to the ITSC’s directory database with an accountability chain that precludes spoofing.
- The ITSCs both maintain the authenticity of the directory database and share/propagate the database among other ITSCs.
- Any user (including those outside the DON) must be able to get the public key of any Naval personnel or command from the database with the confidence that the key is authentic and in accordance with the established trust model.
- Initially, the trust model supported will be similar to that used for military ID cards. Other trust models (such as financial transaction warrants) will be implemented later.

D.4.4.2.8 Configuration Management (CM)

Description: Configuration management will be performed by automated systems throughout the regional ITSCs. The primary purpose is to develop a robust system for managing organizational IT resources. The configuration management system will include inventory information on hardware, software, and associated supporting data. The CM process will support assessment of implementation alternatives, change management, and interoperability. Use of the CM tool should be intuitive, be supported by fill-in-the-blank screens, and be free from cryptic computer syntax. There are other CM functions that are performed within the IT infrastructure (e.g., security, applications) which are addressed under their respective subject areas.

Guidance: At a minimum, ITSC CM services will:

- Implement a standards-based hardware and software inventory.
 - ◆ Consolidate existing hardware and software inventories in a standard RDBMS.
 - ◆ Provide a system with query capabilities.
- Provide a push/pull distribution system to allow centralized identification and issuance of software upgrades.
- Provide centralized administration of:
 - ◆ minimum configurations for determining and initiating required service and
 - ◆ specific service levels based on individual user requirements, including
 - basic IP,
 - telephony,
 - multimedia, and
 - other IT requirements.
- Set minimum requirements for documentation of the CM data maintained, including baseline, changes made, who made the changes, and why changes were made.
- Use a standard tool set across the enterprise with the following features:
 - ◆ Link management devices and management agents with all network monitoring, reporting, and active fault correcting software to develop a standardized interface for data extraction.
 - ◆ Allow integration into asset and service management solutions and be compatible across ITSCs.
- Support comprehensive change management functions, including change simulation, change history, change detection, and notification. This will be done with an automated interface with the ITSC trouble-tracking software for queries.
- Define templates and defaults for most configurations, which will reduce the time needed to perform an upgrade task and ensure correct implementation.
- Ensure that the following CM procedures are consistent across the enterprise, for example, standard CM database fields (Attachment A).
- Define definitions of administrators' permissions precisely. Policies will be uniformly enforced throughout the enterprise, and unauthorized changes will be automatically flagged.

D.4.4.3 ITSC-supported User Services

This section describes the user services that all functional areas require that must be accessible from the network. These network services, as outlined in Figure D-1, are provided by the family of ITSCs and must have a common planning framework and consistent implementation strategy. Some services must be implemented under an enterprise hierarchical plan. These services are fully described in Chapter 4 and are further described in the template in which additional amplification for ITSC implementation may be necessary.

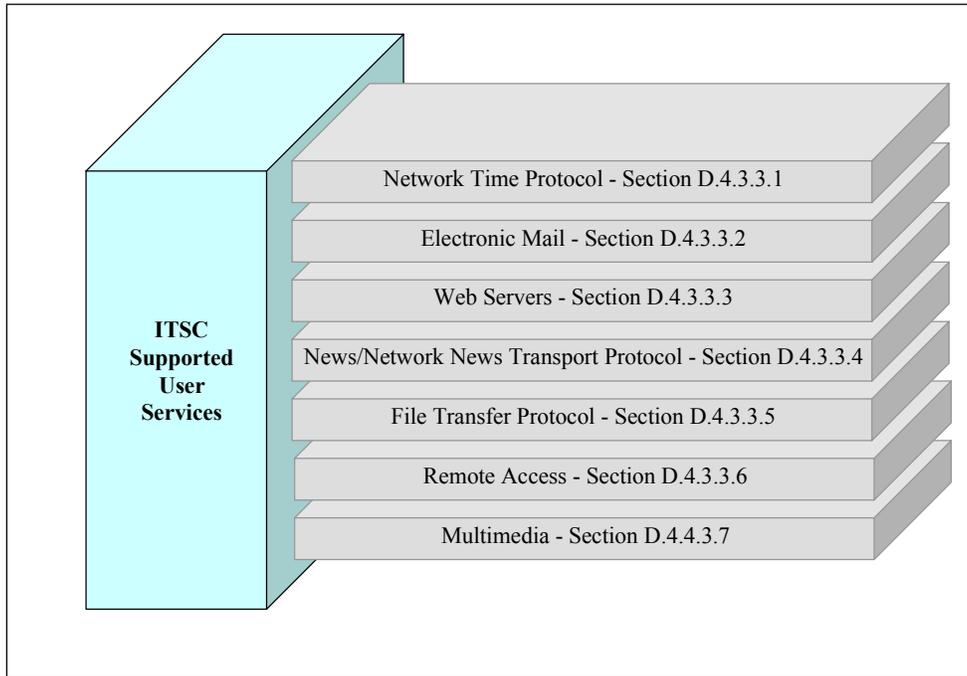


Figure D-1. ITSC Support User Services

D.4.4.3.1 Network Time Protocol (NTP)

Description: NTP services assure accurate local timekeeping so that all servers and services have a consistent time. This is especially important for logging servers, file servers, and some security devices.

Guidance: The NTP service description as provided in Chapter 4 is fully applicable for ITSC implementation.

D.4.4.3.2 Electronic Mail (E-mail)

Description: E-mail is the basic service for interpersonal and organizational messaging which is used throughout the DON. E-mail employs store-and-forward technology that does not provide real-time information exchange, but does provide the capability for high-speed communication of small messages or file transfer. Both individual messaging (E-mail) and organizational messaging (DMS) are supported for the entire Naval enterprise.

Guidance: The E-mail service description as provided in Chapter 4 is fully applicable for ITSC implementation.

D.4.4.3.3 Web Servers

Description: World Wide Web (WWW) service provides one-to-many information sharing throughout the DON and to the public Internet. It is a “pull” technology that allows retrieval (i.e., pull) of shared information from servers. The information is stored in a hypertext transport protocol (HTTP) or eXtended Markup Language (XML) for transport, rendering, and display across an IP network using a WWW browser.

Guidance: The Web Server service description as provided in Chapter 4 is fully applicable for ITSC implementation.

D.4.4.3.4 News/Network News Transport Protocol (NNTP)

Description: NNTP is an information distribution service that provides selective access to “net news.” NNTP varies from an e-mail subscription in that the information content is not stored on “news servers” and is replicated to the degree necessary to provide reasonable local access and performance. Client tools “pull” this content from the news servers and make it available to users for presentation on demand based on the user’s particular selection of “news groups.”

Guidance: The NNTP service description as provided in Chapter 4 is fully applicable for ITSC implementation.

D.4.4.3.5 File Transfer Protocol (FTP)

Description: FTP is used for bulk file upload and download between computers. From a client perspective, a user can connect to a remote computer and either “get” or “put” one or more files as well as perform other simple file manipulation commands. FTP provides a solution for many of the e-mail shortcomings. Large files can be distributed by placing them onto an ftp server and then announcing a pointer to that location so recipients can download needed files at their convenience.

Guidance: The FTP service description as provided in Chapter 4 is fully applicable for ITSC implementation.

D.4.4.3.6 Remote Access

Description: Remote access provides a modem pool for telecommuters, travelers, and other users to dial up and gain access to the DON enterprise. Regional ITSCs cooperate to publish local access numbers for all metropolitan areas in all regions. This permits frequent travelers to dial local numbers for access to the enterprise. Secure remote access through the Internet is also provided.

Guidance: The Remote Access service description in Chapter 4 is fully applicable for ITSC implementation.

D.4.4.3.7 Multimedia

Description: Multimedia services include video teleconferencing (VTC), video applications sharing, video teletraining, and video and image/graphics file servers. Also covered are VTC application enhanced data services that allow users to share applications/documents and to participate in collaborative activities including video applications sharing, video document sharing, and “white boarding.” VTC allows geographically-dispersed personnel and activities to conduct face-to-face meetings in real time through the transmission of images and sound.

Guidance: The Multimedia service description in Chapter 4 is fully applicable for ITSC implementation.

D.5 Hierarchical Service Structure ITSC and ITOC

The services described in this template are intended for execution by the DON ITSC management structure. Determining the way that these services are distributed is not the purpose of this initial DON ITI architecture document, rather, the purpose is to establish ITSC services and a description of those services. Having defined the functions to be performed, it is then appropriate to determine the structure that can best provide those services efficiently, effectively, competitively, and with accountability to the customers. This ITSC organization is a pivotal element in obtaining a world-class DON enterprise network and appropriate, cross-functional input and attention to this decision is expected.

It is obvious that there will be ITSCs in each of the MANs or regions and these will have extension services at the campuses. A description of these extensions, called Information Technology Outreach Centers (ITOCs), is provided. The ITOC functions are not a duplication of the consolidated ITSC functions. For example, an ashore ITOC may be able to view a NOC's network management map on demand, but it cannot generate its own. Importantly, both the command relationship and the required functionality of the ITOC differ depending on whether the ITOC is located ashore or if it is deployed/afloat.

D.5.1.1.1 Ashore ITOCs

Ashore, base Information Technology Outreach Centers (ITOCs) have electronic access to ITSC operations, administration, and service information and have appropriate tools to monitor, diagnose, and correct network problems as well as computer and peripheral hardware problems. Because an ITOC can be expected to serve several commands at a campus, and because of the need for ITSC/ITOC integrity, it is logical that the ITOC be part of the ITSC command

In the case of ashore units, stable connectivity to the ITSC can be assumed, so the ITOC requirement to directly run NOC operations can generally be dispensed in favor of getting the NOC's management picture when needed. This elimination of local 24-hour watch requirements represents a considerable economy. Similarly, end system administration, especially of servers, can be centralized at the ITSC (even if a server is physically located remotely from the ITSC). By contrast, the Help Desk and applications planning functions (both day-time work functions) can be expected to be larger than on deployed units. The ITOC should present an effective Help Desk "human face" to the end user -- the ITOC contact should be able to work seamlessly with the ITSC Help Desk staff to escalate and resolve problems and provide customer feedback.

D.5.1.1.2 Deployed/Afloat ITOCs

Operational units require unit integrity and thus, a significant degree of autonomy and self-sufficiency. Therefore, the ITOC will be part of ship's company. The ITOC capability is a subset of the ITSCs function and generally includes:

- Network management. This is a subset of the NOC capability. In the case of operational units, they operate their own network management system and monitor agents within the command by forwarding a consolidated picture to the ITSC (this is constrained by bandwidth use over radio-WAN). This function generally requires a 24-hour watch standing network management capability while deployed. When a ship is tied up in port and has established

shore-tie network connectivity, it can transfer its NOC watch-standing requirement to the ITSC NOC and secure its own NOC operation.

- End system administration. Both user clients and some servers will be part of a deployed unit's IT organization and will require maintenance in terms of operating system updates, configuration, application software installation, and license management and control. End system administrators will be expected to generate PKI certificates and authentically forward the public key personas to the ITSCs (refer to Chapter 4, PKI, and the directory).
- IT hardware installation, maintenance and troubleshooting. An extreme example is the Marine Corps requirement to set up the IT shop when phasing ashore in expeditionary operations. But even in these relatively more stable installations, additions, changes, and casualty maintenance are required.

D.6 ITSC Infrastructure Physical Attributes

The resultant characteristics of ITSC infrastructure are equally important for the consistency and quality of IT functions and services provided to the Naval enterprise network. The work of world-class service centers must be considered and incorporated to ensure that ITSC support to the Navy and Marine Corps is consistent with mission support expectations.

The standards for power, cooling, security, fire suppression, cable plant, and other related physical characteristics are extensively addressed in the DON ITSG in Chapter 4.

The implementation of ITSCs should not be left to individual discretion or interpretation or to available expertise. One ITSC information source is the National Association of Network Operating Group (NANOG). Information from the NANOG is available at <http://www-personal.umich.edu/~wbn/DataCenterNeedsNotes.htm>.

D.7 Metrics

Selected metrics for the ITSC are outlined in this document and the DON ITSG. Metrics and ITSC are viewed as critical success factors in any DON enterprise solution. Specific feedback from the largest Naval organizations showed a widely-held skepticism that any existing Naval organization could provide an acceptable ITSC service on a world-class basis. For this reason, these organizations are reluctant to align with any enterprise ITSC initiative. Metrics are therefore an important element of describing what specifically is to be provided and a means to ensure that the promised service is delivered.

The cost and performance of the ITSC implementation must be supported by robust metrics that support the ITSG as a best value. The functions of the ITSCs, when established, will be reviewed for alternative sourcing on a regular basis. When performance and cost metrics do not support it, alternatives to performing a function in the ITSC will be evaluated. This is concluded to be an important strategy to avoid substandard service.

Alignment of ITSC services with the needs of all ITSC customers is a primary focus. Metrics should be chosen to provide clear indication of the ability of the ITSC to meet customer requirements instead of the ability to meet internal ITSC priorities.

Industry best practices provide an excellent source for modeling and aligning network services. ITSG Chapter 10.4.6 provides a strategy for selection of the metrics.