Information Technology Standards Guidance

Version 99–1
5 April 1999

Department of the Navy
DON CIO ITSG Integrated Product Team

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

7 Apr 99

MEMORANDUM FOR DISTRIBUTION

Subj: INFORMATION TECHNOLOGY STANDARDS GUIDANCE OFFICIAL RELEASE

With rapidly emerging technologies shifting operations towards electronic processing, representatives from Navy and Marine Corps' operating forces, major claimants and program sponsors have recognized the need for Information Technology (IT) standards in creating an interoperable Naval enterprise information environment. To address this requirement, the Department of the Navy (DON) Chief Information Officer (CIO) Board of Representatives (BOR) chartered the Information Technology Standards Guidance (ITSG) Integrated Product Team (IPT) to collaboratively develop IT standards guidance and direction for the DON enterprise. The IPT's resulting product, the ITSG Version 99-1 document, dated 5 April 1999, has been unanimously approved by the DON CIO BOR and is issued as the information technology standards guidance for the DON.

The ITSG applies to all DON systems that produce, use, or exchange information electronically, and is intended for anyone involved in the management, development, acquisition and operation of new or improved systems. It provides the standards, specifications, best practices and operating profiles required to implement and maintain an integrated, enterprise information infrastructure. It addresses networks, systems, applications, and data in terms of technologies and interrelationships needed to support interoperability across the Department and facilitate scalability to future operations. Enterprise-wide use of these DON IT standards will enable coordinated communications across dispersed DON organizations, and facilitate a smooth transition to twenty-first century naval operations.

All commands in the Navy and Marine Corps are required to consider the standards and guidance in the ITSG to maximize interoperability and enable focused information support across the Department. The ITSG Version 99-1 contains no mandatory requirements, and cannot be used as justification for less than full and open competitive acquisition.

The ITSG is available on the World Wide Web at http://www.doncio.navy.mil/itsgpublic/. At a minimum, it will be updated annually to reflect changes and trends in the IT environment. Please contact Mr. Bob Green at (703) 607-5654/bob.green@hq.navy.mil for general information on the ITSG document, and direct technical issues or questions to Mr. Richard Lynch at (703) 602-6419/lynch.richard@hq.navy.mil.

D. E. Porter

Table of Contents

1. Introduction....1

1.1 Background 1

1.1.1 Establishment of the ITSG....2

1.2 Purpose, Scope and Applicability 3

1.3 Relationship to the JTA and DII COE 4

1.4 Relationship to the DON IM/IT Strategic Plan 4

1.4.1 Network-Centric Environment....4

1.4.2 Client/Server Model of Computing 5

1.4.3 Open System Standards 5

1.4.4 Acquisition Improvement 5

1.4.5 Information Process Re-Invention....6

1.5 Use of the DON ITSG....6

1.6 Document Organization 7

1.7 Promulgation of IT Standards and Guidance....8

1.8 Changes to this Document....9

1.9 Waiver of ITSG Compliance 10

2. Approach to IT Standards Guidance (ITSG)....11

2.1 Best Practices, Standards, Products and Guidance 12

2.1.1 Open System Standards 12

2.1.2 De Facto Standards....14

2.1.3 Product Suite and Products 14

2.1.4 Order of Precedence 14

2.2 Application of Standards and Guidance....14

2.3 Level of Abstraction....15

2.4 System Capability 15

2.5 Standards, Architectures and Infrastructure 16

2.5.1 Supporting Infrastructure Evolution....16

2.5.2 Characterizing Information Technology....18

2.5.3 The Logical Environment 22

2.5.4 Area Network Designations....23

2.5.5 The Physical Environment....27

2.5.6 Information System Domains....28

2.5.7 System Domain Components and Linkages....29

2.6 Platforms, Activities and Operating Environments 30

2.7 Currency of Standards and Guidance 33
2.8 Degree of Compliance 35
2.9 Standards and Guidance Selection Criteria 35
2.10 Enterprise Standards and Guidance Profiles 36
2.10.1 Profiles 36
2.10.2 DOD Technical Reference Model 36
2.11 Promulgation of IT Standards and Guidance 37
2.12 References 38

3. Information Protection 39
3.1 Overview 39
3.2 Background 39
3.3 Information Protection Requirements 40
3.4 Defense in Depth Approach 42
3.4.1 Zone 4 Protection Mechanisms 44
3.4.2 Zone 3 Information Protection Mechanisms 51
3.4.3 Zone 2 Information Protection Mechanisms 53
3.4.4 Zone 1 Information Protection Mechanisms 54
3.5 Public Key Infrastructure 60
3.6 Use of Commercially Available Cryptography 64
3.6.1 Overview of Cryptography 65
3.6.2 Standards for Symmetric Encryption Algorithms 65
3.6.3 Standards for Public Key Cryptography 67
3.6.4 Standards for Message Digest Algorithms 68
3.6.5 Digital Signatures 69
3.7 References 70

4. Facility and Environmental Requirements 75
4.1 Overview 75
4.2 Site Security 76
4.3 Cable Plant 76
4.3.1 Definitions 77
4.3.2 Media 78
4.3.3 Patch Panels, Interconnection Boxes and Connectors 80
4.3.4 Connectors 82
4.3.5 Topology, Security & Integrated Cabling 85
4.3.6 Cable Security 87
4.3.7 Cable Plant Integration Guidance 88
4.3.8 Cable Plant Management 89

4.4 Shipboard Facility Requirements....90
4.4.1 Racks....90
4.4.2 Electrical System Interfaces....92
4.4.3 Air Conditioning....93
4.4.4 Satellite Communication Equipment Requirements....93
4.4.5 Special Considerations for Shipboard Mission Critical Signals....95
4.5 Shore-based Facility Requirements....96
4.5.1 Architectural Components:....96
4.5.2 Fire Protection Components:....96
4.5.3 Mechanical Components:....97
4.5.4 Electrical Components....97
4.6 Ground Combat Environment....97
4.7 Naval Aircraft Environment....98
4.8 References....98
4.8.1 Standards and Specifications Resources....98
4.8.2 Supporting Resources....101

5. Information Transfer....103

5.1 Overview....103
5.1.1 Operational Environment Considerations....104
5.1.2 Adopted Network Definition....105
5.1.3 Performance Issues....106
5.2 Physical and Data Link Layers....109
5.2.1 Local and Metropolitan Area Network Physical and Data Link Layer Technologies....109
5.2.2 Wide and Metropolitan Area Network Physical and Data Link Layer Technologies....121
5.2.3 Radio Communications to Dispersed Forces....124
5.3 Internetwork Protocols....133
5.3.1 ATM....134
5.3.2 Network Layer....135
5.3.3 Transport Layer....137
5.4 Routing and Mobility Protocols....138
5.4.1 Routing....139
5.4.2 Mobile Addressing....141
5.5 Quality-of-Service....142
5.5.1 Description....142
5.5.2 State....143
5.6 References....144
5.6.1 Standards and Specifications Resources....144

5.6.2 Supporting Resources 148

6. Information Distribution 149

6.1 Overview 149

6.2 Concept of Operations for BNIDS 152

6.2.1 Official Individual Accounts 152

6.2.2 Command/Staff Accounts 153

6.2.3 Duty/Watch Accounts 154

6.2.4 Command Correspondence and Distribution Lists 154

6.2.5 Directory Services 155

6.2.6 Defense Message System (DMS) Interoperability 156

6.2.7 Security Certificate and Login Services 159

6.2.8 Web Drop and Pickup Service 159

6.2.9 BNIDS CONOPS Summary 159

6.3 Domain Name and Directory Services 160

6.3.1 Domain Name Service (DNS) 160

6.3.2 Directory Service 162

6.4 Public Key Infrastructure (PKI) 164

6.5 Electronic Messaging and Attachments 165

6.5.1 Implementation Guidance 167

6.5.2 Selection of an E-mail System 167

6.5.3 E-mail System Implementation 168

6.5.4 Interoperability with Other E-mail Systems 168

6.5.5 Individual's Official E-mail Address 169

6.5.6 Display Name 169

6.6 Network Utility Services 169

6.6.1 Network Time Service 169

6.6.2 System Management Services 171

6.6.3 Remote Access Services 172

6.6.4 File Transfer Services 172

6.6.5 Electronic Dialog 174

6.7 Web Services 174

6.7.1 Web Servers 174

6.7.2 Web Browsers 175

6.7.3 Web Utilities 181

6.7.4 Data Search and Retrieval 182

6.7.5 Data Push 184

6.8 Network News Service 186

6.9 References 187

6.9.1 Standards and Specifications Resources 187

7. Computing Resources 189

7.1 Overview 189
7.1.1 Background 189
7.1.2 Scope of Computing Resources 190
7.1.3 General Philosophy 190

7.2 Computing Hardware 193
7.2.1 Component Technologies 193
7.2.2 System Configurations 201

7.3 Operating System Services 208
7.3.1 Operating Systems 208
7.3.2 Application Programming Interface 219
7.3.3 Human Computer Interface 220

7.4 Operating Considerations 223
7.4.1 Security 223

7.5 Communications 223
7.5.1 Real Time 224
7.5.2 High Availability 224

7.6 References 225
7.6.1 Standards and Specifications Resources 225
7.6.2 Supporting Resources 229

8. Information Management 231

8.1 DOD Policy 233
8.1.1 Information Interoperability 233
8.1.2 Information Management 233
8.1.3 Data Administration 234

8.2 Information Architecture 235

8.3 Information Interchange 238
8.3.1 Push versus Pull 238
8.3.2 Information Discipline 240
8.3.3 Data Interchange Services 242
8.3.4 Messages 256

8.4 Database Management 258
8.4.1 Database Management Process 258
8.4.2 Database Interoperability 261
8.4.3 Database Documentation 265
8.4.4 Database Management Systems 266

8.5 Data Quality and Interoperability Metrics 273
8.5.1 Data Quality versus Information Quality 273

8.5.2 Data Interoperability 273
8.5.3 Database Assessment Areas 274
8.5.4 Selecting Performance Metrics 274
8.6 Information Engineering Tools 276
8.6.1 Process Modeling Tools 276
8.6.2 Data Modeling Tools 277
8.6.3 Information Transfer Management Tools 277
8.6.4 Architecture Management Tools 277
8.6.5 GOTS Information Tool Descriptions 278
8.7 References 281

9. Applications 285

9.1 Overview 285
9.1.1 Background 285
9.1.2 Defense Information Infrastructure Common Operating Environment (DII COE) 287
9.1.3 Beyond Software 288
9.1.4 Outline 288
9.2 Common Support Applications 289
9.2.1 Office Automation 289
9.2.2 Multimedia Information Processing 290
9.2.3 Interpersonal Communications 291
9.2.4 Environment Management 292
9.2.5 Database Utilities 293
9.2.6 Graphics and Imaging 293
9.2.7 Engineering Support 295
9.3 Cooperative Work Applications 295
9.3.1 Electronic Forms 298
9.3.2 Workflow Management 298
9.3.3 Conferencing 299
9.3.4 Calendaring and Scheduling Systems 300
9.3.5 Group Decision Support Systems 300
9.4 Computer Telephony 300
9.4.1 Computer Telephony Integration (CTI) 301
9.5 Video Teleconferencing 302
9.5.1 Afloat Video Teleconference Systems 302
9.5.2 Shore Video Teleconference Systems 303
9.5.3 Security 305
9.5.4 Video Networks and Services 306
9.5.5 Video Recommended Standards Summary 307

9.6 Mission Area Applications 310
9.7 Application Support Services 311
9.7.1 General Software Engineering Services 311
9.7.2 Web Development 311
9.8 References 313

10. Enterprise Management 319
10.1 Introduction 319
10.2 Organizing for Enterprise Management 321
10.2.1 Enterprise Management 321
10.2.2 Concept of Operations 326
10.3 System Monitoring and Control Standards Guidance 329
10.3.1 The X.700 Series and XSM 331
10.3.2 Industry Specifications 333
10.4 System Quality 337
10.4.1 System Quality Concept 338
10.4.2 System Effectiveness 340
10.4.3 System Efficiency 347
10.4.4 System Characteristics 351
10.4.5 System Behavior 355
10.4.6 Selection of Performance Metrics 358
10.5 References 358

List of Figures

Figure 1-1. ITSG Document Map Highlighting Chapter 1, Introduction 1
Figure 1-2. ITSG Document Map 7
Figure 1-3. Generic ITSG Chapter Outline 9
Figure 1-4. ITSG Change Process 10
Figure 2-1. ITSG Document Map Highlighting Chapter 2, Approach to ITSG 11
Figure 2-2. Transition of Information Technology 17
Figure 2-3. Operator's Perspective of the Information Infrastructure 19
Figure 2-4.System Manager's Perspective of the Information Infrastructure 20
Figure 2-5. ITSG Information Technology Categories 21
Figure 2-6. Logical Infrastructure Model 23
Figure 2-7. Comparison of Area and Virtual Private Networks (VPNs) 25
Figure 2-8. Adopted Architecture Model for LANs, MANs, WANs, and Radio Communication to Dispersed Forces 26
Figure 2-9. Global Infrastructure Model 27
Figure 2-10. Information System Domain 29
Figure 2-11. System Domain Components and Linkages 30
Figure 2-12. Information Technology Service Center 31
Figure 2-13. Operating Environment Matrix 33
Figure 2-14. Technology Life Span 34
Figure 2-15. Sample ITSG Implementation Time Line 35
Figure 2-16. DoD Technical Reference Model (Version 3.0) 37
Figure 2-17. Generic ITSG Chapter Outline 38
Figure 3-1. ITSG Document Map Highlighting Chapter 3, Information Protection 39
Figure 3-2. Information Protection Summary 42
Figure 3-3. Defense in Depth Concept 43
Figure 3-4. Security Components Applied to Architecture Dimensions and Protection Zones 44
Figure 3-5. Allowable Services for Network Firewalls 48
Figure 3-6. Example Certificate Issuance Process 62
Figure 3-7. Example Certificate Revocation Process 63
Figure 4-1. ITSG Document Map Highlighting Chapter 4, Facility and Environmental Requirements 75
Figure 4-2. RJ-45 Pin Specifications for T-568A 84
Figure 4-3. SATCOM Nominal Physical Characteristics 94
Figure 5-1. ITSG Document Map Highlighting Chapter 5, Information Transfer 103
Figure 5-2. Adopted Architecture Model for LANs, MANs, WANs, and Radio Communication to Dispersed Forces 106
Figure 5-3. Evolution of LAN and WAN Data Throughput 107
Figure 5-4. ISO/OSI model layers 1 and 2 109

Figure 5-5. Summary of Lower Layer Networking Technology....111
Figure 5-6. RF Bands Used in SATCOM....125
Figure 5-7. ISO/OSI Model Layers 3 and 4....133
Figure 6-1. ITSG Document Map Highlighting Chapter 6, Information Distribution....149
Figure 6-2. ISO/OSI Model Layers 5 - 7+....149
Figure 6-3. Basic Network and Information Distribution Services (BNIDS) Showing the Order of Discussion....150
Figure 6-4. User-Centric View....153
Figure 6-5. X.500 Directory Update and Maintenance....155
Figure 6-6. DMS Multi-Function Interpreters....157
Figure 7-1. ITSG Document Map Highlighting Chapter 7, Computing Resources....189
Figure 7-2. ISO/OSI Model and the Computing Environment....189
Figure 7-3. Computing Resources in the Context of the DOD Technical Reference Model....190
Figure 7-4. Three-Tiered Application Architecture....191
Figure 7-5. Rationale for the DON enterprise client-server strategy....192
Figure 7-6. Personal Workstation Configuration Summary....203
Figure 7-7. Remote Procedure Call....213
Figure 7-8. Message Passing....218
Figure 7-9. Message Queuing....218
Figure 7-10. HCI Development Guidance....221
Figure 8-1. ITSG Document Map Highlighting Chapter 8, Information Management....231
Figure 8-2. Relationship Between Information Management, Information Infrastructure, and Operations....232
Figure 8-3. Information Management in the Context of the DOD Technical Reference Model....233
Figure 8-4. Information Requirements Definition....236
Figure 8-5. Information Architecture....236
Figure 8-6. Information Dissemination Architectures....238
Figure 8-7. Development Approach....258
Figure 8-8. Information Improvement Process....260
Figure 8-9. Methodology for Achieving and Maintaining DON Information Interoperability....262
Figure 8-10. Capturing Metadata in a Common Format....262
Figure 8-11. Data Element Table....263
Figure 8-12. Data Element Description....263
Figure 8-13. Data Element Comparison and Linking....264
Figure 8-14. Database Synchronization....265
Figure 8-15. Guidelines for Selecting a DBMS Model....267
Figure 8-16. The Open Group SQL and RDA....268
Table 8-17. LISI Reference Model....275
Figure 9-1. ITSG Document Map highlighting Chapter 9, Applications....285
Figure 9-2. Applications in the Context of the DOD Technical Reference Model....286

Figure 9-3. Three-Tiered Application Architecture....287
Figure 9-4. Forms of Groupware....296
Figure 9-5. Overlap Between Groupware, The World Wide Web, and Usenet....297
Figure 9-6. Desktop Video Configuration for Supporting Dial-up Classified and Unclassified Conferencing....305
Figure 9-7. DVS-G Video Network Architecture....306
Figure 10-1. ITSG Document Map highlighting Chapter 10, Enterprise Management....319
Figure 10-2. Enterprise Management Standards and Guidance in the context of the enterprise system architecture....320
Figure 10-3. Matrix of Enterprise Management Functions, System Component Categories and Geographic Coverage....326
Figure 10-4. ITSC Functions Including Enterprise Management, Interface and Centralized Computing Services....327
Figure 10-5. ITSC Information Technology Management Tools....329
Figure 10-6. X.700 Series Specifications and Related ITU Proposals....333
Figure 10-7. SNMP, RMON 2, WBEM and DMI relationship to the ITSC Information Technology Management Tools....334
Figure 10-8. Systems quality dimensions....339
Figure 10-9. Relationship Between Mission and Infrastructure Effectiveness....341
Figure 10-10. Aggregation of Costs to Provide the Total Cost of Ownership....349
Figure 10-11. Summary of System Quality Measurements....354

List of Tables

Table 3-1. Zone 4 Firewall Recommended Implementations 46
Table 3-2. Zone 4 VPN Implementations 50
Table 3-3. Zone 4 Content Security Checking Implementations 51
Table 3-4. Zone 4 Routing Table Security Implementations 51
Table 3-5. Zone 3 Network Intrusion Detector Implementations 52
Table 3-6. Zone 2 Network Access Controller Implementations 54
Table 3-7. Operating System Security Implementations 56
Table 3-8. Data at Rest Encryption Implementations 56
Table 3-9. E-mail Encryption Implementations 58
Table 3-10. WWW Encryption Implementations 59
Table 3-11. Content Security Checking Implementations 60
Table 3-12. Public Key Infrastructure Implementations 64
Table 3-13. Symmetric Encryption Algorithm Implementations 67
Table 3-14. Public Key Cryptography Implementations 68
Table 3-15. Message Digest Algorithm Implementations 69
Table 3-16. Digital Signature Implementations 70
Table 4-1. Cable Media Recommended Implementations for Ships 77
Table 4-2. Cable Media Recommended Implementations for Shore and ITSC Use 77
Table 4-3. Patch Panels, Interconnection Boxes and Connectors Recommended Implementation for Shipboard Use 81
Table 4-4. Patch Panels, Interconnection Boxes and Connectors Recommended Implementation for Shore and Base Use 81
Table 4-5. Topology, Security, Cable Integration Recommended Implementations 85
Table 5-1. Data Rate Designations 108
Table 5-2. Physical and Data Link Recommended Implementations for LANs 110
Table 5-3. Physical and Data Link Recommended Implementations for WANs 121
Table 5-4. Physical and Data Link Recommended Implementations for Radio Communications to Dispersed Forces 125
Table 5-5. Network and Transport Layer Recommended Implementations 134
Table 5-6. Network Routing Protocol Recommended Implementations 139
Table 5-7. Quality of Service Recommended Implementations 142
Table 6-1. Interim DMS Interoperability with the DON Information Infrastructure 158
Table 6-2. Naming Services Standards 161
Table 6-3. Directory Service Recommended Implementations 162
Table 6-4. X.400 Address Attributes 164
Table 6-5. E-mail with Attachments Recommended Implementations 167
Table 6-6. Standard User Directory Fill 168
Table 6-7. Network Time Service Recommended Implementations 171
Table 6-8. System Monitoring and Control Recommended Implementation 172

Table 6-9. File Transfer Service Recommended Implementations 173
Table 6-10. Web Service Recommended Implementations 175
Table 6-11. Web Client Recommended Implementations 178
Table 6-12. Network News Standard 186
Table 7-1. CPU Recommended Implementations 194
Table 7-2. Bus Standards 195
Table 7-3. Memory (RAM) Standards 196
Table 7-4. I/O Interface Standards 197
Table 7-5. Storage Device Media 200
Table 7-6. Disk RAID Levels 201
Table 7-7. Personal Workstation (Portable) Hardware Configuration Guidance 202
Table 7-8. Personal Workstation (Desktop) Hardware Configuration Guidance 202
Table 7-9. Server Hardware Configuration Guidance 206
Table 7-10. Enterprise Computing Hardware Configuration Guidance 207
Table 7-11. Embedded Computer Systems Hardware Configuration Guidance 208
Table 7-12. Personal Workstation Operating Systems 209
Table 7-13. Server Operating Systems 210
Table 7-14. Enterprise Computer Operating Systems 211
Table 7-15. Remote Procedure Call 214
Table 7-16. File Service 216
Table 7-17. Object Service 217
Table 8-1. Data Administration Implementation 235
Table 8-2. Information Architecture Implementation 237
Table 8-3. Document Exchange Standards 244
Table 8-4. File Formats 245
Table 8-5. Digital Technical Data Standards for Technical Manual Creation. 246
Table 8-6. Graphics Standards for Technical Manual Creation. 246
Table 8-7. Digital Technical Data Standards for Legacy Data Conversion 247
Table 8-8. Geospatial Service Standards 249
Table 8-9. Imagery Service Standards 250
Table 8-10. Product data interchange standards 253
Table 8-11. Product Data Creation 253
Table 8-12. Atmospheric Data Interchange Standards 255
Table 8-13. Oceanographic Data Interchange Standards 256
Table 8-14. Bit-Oriented Message Standards 257
Table 8-15. Character-Oriented Message Standards 257
Table 8-16. DON Information Management Implementation 261
Table 8-17. DON Data Base Documentation Guidance 266
Table 8-18. Relational Database Management Systems 268
Table 8-19. Object-oriented database management systems 269
Table 8-20. Database access 270

Table 8-21. Data Quality and Data Interoperability Perfromance Metrics Implementation.....276
Table 9-1. Data delivery: application programming interfaces.....291
Table 9-2. Data delivery: application programming interfaces.....294
Table 9-3 3-D Computer Graphics.....295
Table 9-4 Computer telephony integration.....302
Table 9-5 Video Standards Overview Matrix.....309
Table 9-6 Video Standards.....310
Table 9-7. Web Development Standards.....313
Table 10-1. Enterprise Management Functions.....322
Table 10-2. System Monitoring and Control Recommended Implementation.....331
Table 10-3. Dimensions of System Quality.....340
Table 10-4. System Quality Metrics Summaries (format).....340
Table 10-5. System Performance Metrics Summary.....344
Table 10-6. Information Quality Metrics Summary.....347
Table 10-7. System Efficiency Metrics Summary.....351
Table 10-8. System Characteristics Metrics Summary.....355
Table 10-9. System Behavior Metrics Summary.....357

1. Introduction

The Department of the Navy (DON) Information Technology Standards Guidance (ITSG) identifies the standards and provides the guidance for applying information technology toward the creation and sustainment of a responsive, and user-friendly, information management environment. All commands in the Navy and Marine Corps are required to consider the standards and guidance herein to maximize interoperability and focused information support.

As a guide, each chapter will begin with the following map (Figure 1-1) and a description of its relationship to the rest of the document. This chapter, for example, provides the background, purpose, and outline of the ITSG.

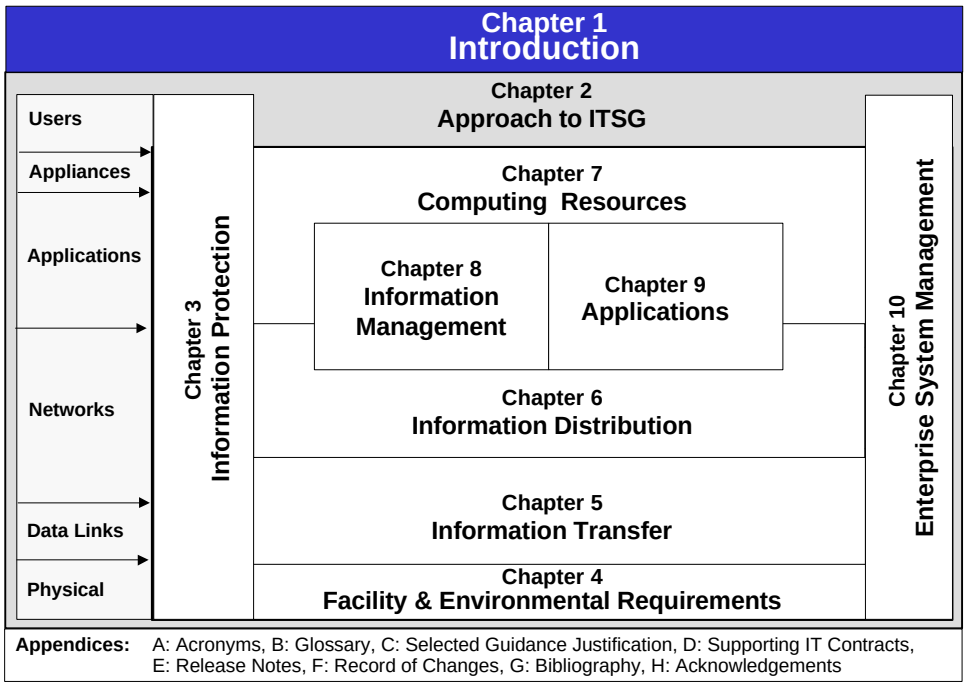


Figure 1-1. ITSG Document Map Highlighting Chapter 1, Introduction

1.1 Background

In the past, our individual commanders in the Department of the Navy (at every level of the organization) built information infrastructures that supported their individual missions. These independent efforts produced a myriad of locally effective solutions. Fleet and Marine Corps concentration areas had a proliferation of communications networks, many in close proximity but each one completely isolated. Functional mission commanders deployed multiple systems often with separate, dedicated transmission systems. Weapon systems on our ships each had their own sensor system and a separate communications system to send data back to the shooter. Our networks were “stovepiped” – they were neither inter-connected nor interoperable.

Joint Vision 2010 states “the unqualified importance of access to information through improvements in the speed and accuracy of transferring data.” The Chief of Naval Operations stated that “interactive connectivity will be required at all levels of the chain of command.” The Commandant of the Marine Corps stated “we must reach and execute effective military decisions

faster than our adversaries through a command and control system that is flexible and adaptable." A Fleet Commander in Chief stated that "a robust information infrastructure and information dissemination to dispersed forces are key elements in achieving information superiority."

The Secretary of the Navy established the position of the Department of the Navy's (DON) Chief Information Officer (CIO) to develop and implement a comprehensive information infrastructure that supports the Naval mission within the Defense Information Infrastructure (DII). A strategy for introducing, fostering and maintaining an effective information technology (IT) environment, as well as integrating and managing information systems, including the information itself, is critical to this endeavor. The goal is to provide complete and timely access to information through an infrastructure that provides interconnectivity, access to information, and tools that allow the Navy and Marine Corps to obtain a competitive advantage and increased productivity.

Providing the "right information to the right people at the right time" depends upon a complete information management construct – process improvement, data management and advanced information technology. All three must be focused on enterprise customers' requirements. The DON IT infrastructure must support interactive connectivity at all levels of the chain of command – national, theater, local, and unit. Our marines, sailors, and civilians must have seamless, robust, and secure access to information.

The Secretary of the Navy has delegated to the DON CIO the responsibility and authority to develop the policy, standards, guidance, and strategy necessary to create and sustain a living information infrastructure. This infrastructure must support the implementation of the DII within the highly dynamic environment that characterizes Naval operations. Unlike commercial industry where organizations and facilities are at fixed locations and the organizational staff is relatively stable, the Navy and Marine Corps environment involves:

- Entire organizations that move between satellite footprints, from sea to port, and from port to port on a routine basis
- Staffs that frequently deploy, embark, and split
- Information system support personnel who rotate biennually

The similarity between military organizations and commercial organizations, however, is that each must deal with changing information technology that causes rapid obsolescence of the infrastructure and allows adversaries or competitors to obtain an advantage. Information technology advancements also place a stress on enterprise interoperability as products are acquired from multiple vendors with advanced, but incompatible, features. The challenge of the DON CIO is to tap the dramatic advancements being made by commercial industry in information technology and guide their continual incorporation into the DON's dynamic and diverse enterprise operating environment.

1.1.1 Establishment of the ITSG

To meet this challenge, the approved DON CIO operational model is based on collaborative centralized planning and decentralized execution. The model creates and empowers a DON CIO Board of Representatives, chaired by the DON CIO, with membership from across the Navy and Marine Corps' operating forces, major claimants, and program sponsors. It establishes DON CIO Integrated Product Teams (IPTs), also with DON-wide presence, which develop enterprise

Information Management and Information Technology (IM/IT) plans, architecture, and standards for the Department.

A series of recent laws, including the Clinger-Cohen Act of 1996 (Public Law 104-106, 1996), require the DON CIO to "develop, maintain, and facilitate the implementation of a sound and integrated enterprise architecture and standards" (Section 5125 (b) (2)). To provide a focus for these efforts, the Secretary mandated that the DON CIO IPTs be the only authorized entities in the Department to develop enterprise IM/IT architecture and standards. All existing or similar efforts in the DON will be consolidated, aligned, or disestablished in order to provide the required focus and effectiveness of the DON CIO efforts.

During its first meeting in May of 1997, the DON CIO Board of Representatives determined IM/IT standards to be its top priority. The Board authorized the stand up of the DON Information Technology Standards Guidance IPT to select and publish a DON Information Technology Standards Guidance (ITSG) document.

This document results from the collaborative efforts of the DON IT Standards Guidance IPT. The IPT was formed using a skills-based approach and is comprised of DON military and civilian technical experts who represent specific IT areas. Each is a Subject Matter Expert (SME) for a particular information technology area and provides expertise, continuity, and accountability for the DON IT standards-related decisions in that area. This approach provides the DON with an improved ability to address the complex technical issues of IT specifications, standards, and operational interfaces.

1.2 Purpose, Scope and Applicability

The purpose of the DON ITSG is to provide specific complementary guidance to support the special IT requirements of Naval organizations complementary to the Joint Technical Architecture (JTA). It is to identify the full complement of best practices, standards and guidance that support full interoperability and seamless interconnectivity within the DON and with the DoD, Federal, and Public Domains. Specifically:

- To provide the foundation for integration, interconnection, and interoperability between and among all tactical, strategic, and sustaining base systems, in-garrison and deployed, ashore and afloat; that produce, use, or exchange information electronically.
- To provide information system security guidance that ensures Naval information system implementation meets DOD security policy.
- To promulgate standards and guidelines for system development and acquisition to significantly reduce lifecycle cost, shorten development and fielding time, and optimize the impact on program financial and execution performance.
- To introduce guidance for measuring the effectiveness and efficiency of the Naval enterprise information infrastructure.

The ITSG must be considered by all DON organizations for IT planning, acquisition, contracting, and operations. Within the ITSG, there are levels of adherence (and freedom) which provide appropriate latitude to meet operating environments and mission requirements while maintaining the goal of interoperability and security. These levels are discussed in Section 2.8. The ITSG applies to all systems that produce, use, or exchange information electronically, and is intended

for anyone involved in the management, development, acquisition and operation of new or improved systems.

1.3 Relationship to the JTA and DII COE

The ITSG complements the JTA and provides additional guidance towards applying the JTA and DII COE to all IT/IM-related systems in the DON. Where the ITSG conflicts with the JTA, the JTA supersedes the ITSG for those systems/interfaces that fall within the scope and applicability of the JTA.

1.4 Relationship to the DON IM/IT Strategic Plan

The DON IM/IT Strategic Plan emphasizes that sound DON information systems architecture and technology standards are essential toward improving Navy and Marine Corps functional mission performance, and promoting greater IT cost-effectiveness. The architecture provides the context to support the functional work processes, information flows, supporting IT systems and infrastructure. The standards provide the specifications and interfaces needed to interface components of the architecture. Together, the architecture and standards help support a DON corporate virtual information infrastructure within the DII to connect every DON IT user. This leads to a condition in which users are given access to common information and information tools empowering them to develop and incorporate new processes. The subsequent improvement in productivity and efficiency enables the “Revolution in Military Affairs” (RMA) and the “Revolution in Business Affairs” (RBA). (See the reference “Mazarr, U.S. Army War College” in Section 1.8 for a description of RMA.)

Principal strategic elements to be supported by the DON ITSG include the following:

- Network Centric Environment
- Client/Server Model of Computing
- Open System Standards
- Acquisition Improvement
- Support for Re-Invention

1.4.1 Network-Centric Environment

A network-centric strategy is an approach that both complements and promotes traditional client/server applications. The DII and the Internet provide significant business value to the DON by providing a ready-made infrastructure for network connectivity. It allows rapid sharing of information, dynamic applications deployment, and leveraged network operations. The Internet protocol suite has enabled the explosion of portable Internet applications.

The network centric strategy adapts and extends Internet technology and infrastructure to meet the DON needs by providing the following:

- Scaleable Internet technology – from room-sized to global networks.

- Leveraging of commercial technology.
- Shareable solutions – best practices solutions can be used DON-wide.
- Supporting “network-ready” systems and information sources early in their design.
- Recognition of diverse operating environments and contingencies
- Understandable basis for corporate direction.

1.4.2 Client/Server Model of Computing

Broken into its basic components, the client/server model includes the network, data servers, application servers, presentation clients, end systems, and associated interfaces. At the border of the network, regardless of its size, are the presentation clients and end systems. The presentation clients consist of personal workstations that include laptop and desktop personal computers (PCs) as well as video teleconferencing (VTC) equipment. End systems consist of the sensors (e.g., radar), communication devices (e.g., telephones), and action devices (e.g., machinery and weapons control) that attach to the network. For this model to perform in a standardized and scaleable fashion, the interfaces must satisfy two basic criteria:

- Data element standardization between the end systems.
- The interface between end systems and the network must be standardized.

The client/server model is generally characterized by the division of an application into components providing the capability for each component to run on different networked computers. This division of work permits components to be positioned to increase the reliability and agility needed for an integrated system to support multiple missions.

1.4.3 Open System Standards

Open system standards are embraced as the desired goal for the DON; however, there are many areas in IM/IT implementation that are not supported by such standards. Guidance, de facto standards, and best practices must be included in the ITSG to support full IT/IM architecture integration. Often there are multiple standards that apply to a single information function. This document presents all guiding elements needed for full information infrastructure integration.

1.4.4 Acquisition Improvement

Actual investments in information technology in the Navy and Marine Corps exceed $2 billion annually. IT investment decisions are made by program managers and unit commanding officers spending their own command budgets to implement independent IT solutions. It is not the intent here to mandate either central procurement activity or central oversight. However, DON commanders and program managers cannot simply develop independent IT acquisition plans, if a seamless, interoperable network is to be built.

For both affordability and innovation, the ITSG supports the use of commercial products in the acquisition process. The standards established in this document represent DON corporate guidance for making decentralized investment decisions about information technology products

and services. It can guide multiple programs and multiple commands to contribute to the larger Navy-Marine Corps enterprise IT solution.

1.4.5 Information Process Re-Invention

Every DON IM/IT process must directly link to and support the established DON mission, goals, and objectives. Information processes that are tied to strategic drivers — linked to critical missions and extensive resources – will receive greatest emphasis for re-invention. While process re-invention will be explored prior to application of IT, the leveraging effects of IT must be emphasized. These efforts, consistent with those described in Joint Vision 2010 and the Quadrennial Defense Review (QDR), will reduce cost while seeking RMA levels of return on investment (ROI). The DON must make the attendant investments in technology refreshment that involve replacing system components and retraining people. This includes introducing new methodologies to prevent or delay obsolescence and exploit new capabilities.

1.5 Use of the DON ITSG

Industry studies support the premise that a coherent corporate technology policy helps an enterprise realize up to 30 percent greater value in productivity, cost control, and decision making. It follows that a corporate information technology policy will also translate into more effective warfighting capability such as speed of command and information superiority needed for dominant maneuver, precision engagement, focused logistics, and full-dimension protection under the Joint Vision 2010 concept.

This document establishes DON guidance as a basis for making daily technology-related decisions across the enterprise, and for planning future system capabilities. As such, it is intended to guide and influence implementation plans. Individual command plans require IT solutions that best support their specific command needs. These plans should include the guidance from this document and a migration strategy that considers their existing information infrastructure.

As an aid to IM/IT planning, the DON ITSG guides the acquisition and development of systems to support new and emerging functionality and provides a target towards which existing systems will move. It is not a catalog of all information technology standards used within today's DON systems. Rather, it represents those standards, specifications, and practices that should be used now and in the future.

The ITSG contains no mandatory requirements and cannot be used as justification for less than full and open competitive acquisition. Purchasing agents and contracting officers continue to be responsible for appropriate source selection and price reasonableness decisions. The use of existing contractual instruments, which have already been competitively awarded, is encouraged because they greatly facilitate the ordering process. Refer to Appendix D of this document for information on available competitively awarded contracts.

This document is based upon a "snapshot" of the current state of technology. This information will be promulgated from the DON CIO Web site which will be frequently updated. The printed document cannot stay as current as the on-line version, but it offers greater portability. Periodic releases of this document will be published to maintain currency, along with release notes (to be reflected in Appendix E) that highlight significant changes. The description and location of specific changes, along with the associated rationale, will also be provided in Appendix F.

1.6 Document Organization

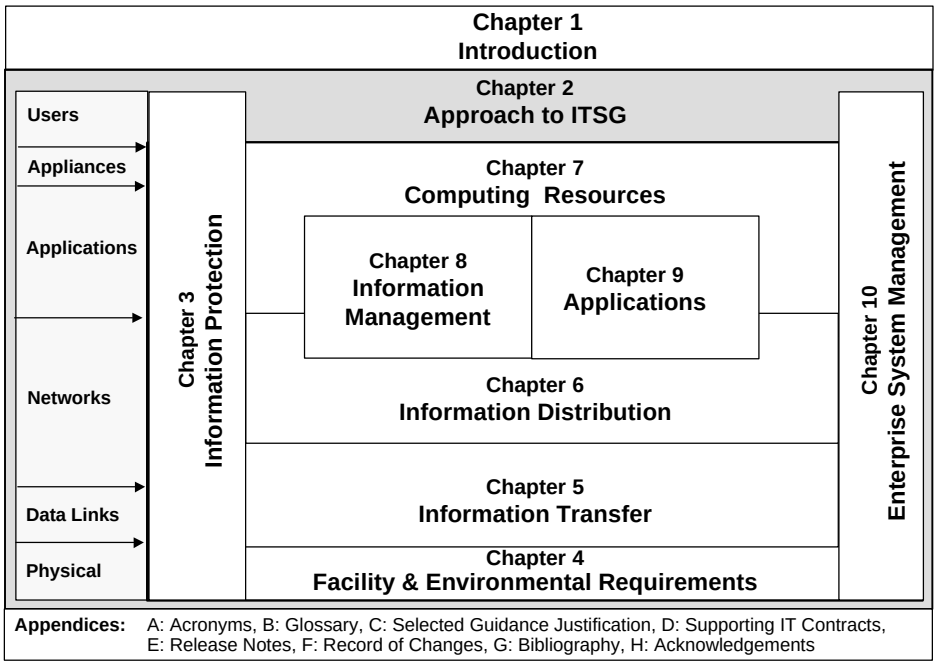


Figure 1-2. ITSG Document Map

Figure 1-2 is a document map of the ITSG which will be provided at the beginning of each chapter for perspective. As shown, this document consists of ten chapters and eight appendixes. The first two chapters provide the background, overview, and approach to establishing the ITSG:

Chapter 1 – Introduction provides the background, purpose, and outline of the document.

Chapter 2 – Approach to the ITSG provides the basis for the organization and selection of guidance.

The remaining eight chapters describe the standards and guidance for a sequence of technology areas:

Chapter 3 – Information Protection includes system and information security standards and guidance.

Chapter 4 – Facility and Environmental Requirements includes cabling, mechanical, and electrical standards and guidance.

Chapter 5 – Information Transfer includes network communication standards and guidance for local area networks, wide area networks, satellite communication networks, end-station connectivity and the internetworking protocols to link these together to form a single information infrastructure.

Chapter 6 – Information Distribution includes core network applications common to all users including electronic mail, web services, time services, file transfer, and directory services.

Chapter 7 – Computing Resources includes computers and associated operating systems, peripherals, and communication devices.

Chapter 8 – Information Management includes the format, structure, organization, and interchange of data within and between information bases.

Chapter 9 – Applications includes software programs that support business and operational applications. Also includes video teleconferencing (VTC) and telephony over data networks.

Chapter 10 – Enterprise Management includes systems management, organization, system monitoring and control, network management and proposed measures of effectiveness for the information infrastructure.

Within each of these chapters is a chapter overview, a description of each technology, and then the associated DON best practices, standards, and guidance including an expected time span of applicability. Each chapter also provides recommendations on how these standards and guidance should be applied to various platforms and facilities.

Eight appendices are provided to include: an acronym list (Appendix A), a glossary (Appendix B), selected guidance justification (Appendix C), supporting IT contracts (Appendix D), release notes (Appendix E), record of changes from the previous version (Appendix F), a bibliography/reference list (Appendix G) and acknowledgments (Appendix H).

1.7 Promulgation of IT Standards and Guidance

Figure 1-3 illustrates how each chapter is organized. As shown, there will be an overview that provides a summary of what is contained in the chapter. Some chapters will also have a background section to provide a foundation to understand the contents. Within the body of the chapter, topics will be introduced and discussed. An associated statement on the implementation of the standard, specification or guidance will be followed by a table showing the recommended implementation over time for different platforms and facilities. Each chapter will close with a list of references. The official references of the standards and guidance will be provided as well as any sources supporting the chapter.

Overview

Background

Topic

Description

Discussion

Best Practices

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Avoid selecting any of these specifications, products, or technologies	Select specifications, products, or technologies based on this time line.				These specifications, products, or technologies are being monitored as potentially significant.
Facilities, Platforms, Operational Environments	The specifications, products or technologies above apply to these platforms or operational environments.				

Notes

References

Sources for Standards Guidance

Supporting Resources

Figure 1-3. Generic ITSG Chapter Outline

1.8 Changes to this Document

This document will be updated periodically by the DON IT Standards Guidance IPT. The process for submission and approval of changes is shown in Figure 1-4. Requirements and/or recommendations should be submitted in writing to the IPT by any organization. The IPT will obtain required input for evaluation, determine appropriate action and review, and provide the recommended action to the DON CIO Board of Representatives. Editorial and minor changes to the document will be approved by the IT Standards Guidance IPT; the Board will approve substantive changes. Following approval, promulgation will include appropriate media products with document management performed by the Office of the DON CIO Staff. Routine change requests will be aggregated and addressed in a semi-annual IPT forum; emergent requirements will be addressed by an electronic IPT and Board of Representatives process. Proposed changes should be provided to the Office of the DON CIO – Enterprise Architecture and Standards Competency. Changes will be presented to the DON IT Standards Guidance IPT for resolution.

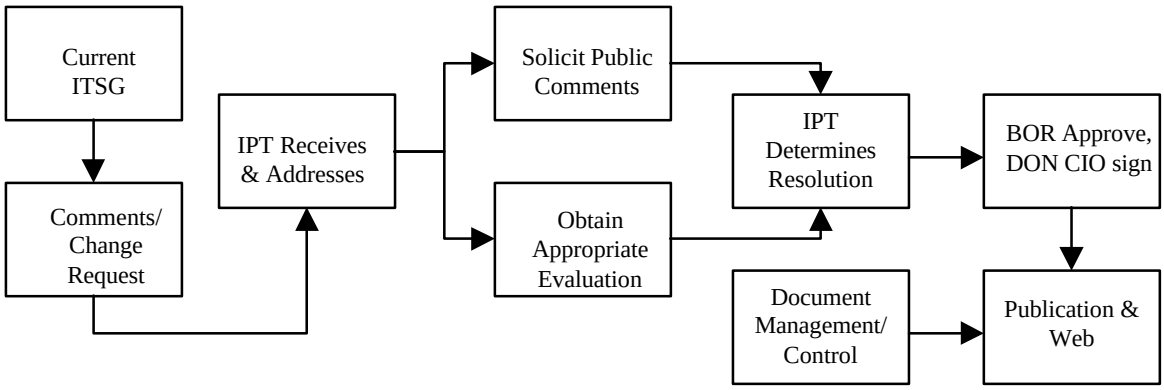


Figure 1-4. ITSG Change Process

The ITSG document will be published annually on CD-ROM to capture standards and guidance updates that have been selected by the IPT and approved by the DON CIO Board of Representatives during the year. Because this document promulgates the entire scope of standards and guidance, it runs the risk that significant portions will be obsolete by the time of publication. During the twelve months between updates, the currency of the printed document will further degrade. The primary source of the ITSG will be a web file that is reviewed and updated quarterly. The URL for the ITSG is www.doncio.navy.mil/itsgpublic.

1.9 Waiver of ITSG Compliance

Responsibility for compliance with this document rests with individual DON organizations. The process by which this is implemented is open to each organization's discretion. It is recommended that each acquisition process be certified by the organization CIO to ensure that contemplated items, services, or processes are in compliance with this document. It is recommended that exceptions be approved in writing by the organization CIO, commanding officer or equivalent. It is further recommended that these exceptions be forwarded to the ITSG IPT as input for further document changes based upon organizational user requirements. Such organization submissions should be forwarded to the DON CIO, Enterprise Architecture and Standards Competency.

2. Approach to IT Standards Guidance (ITSG)

This chapter provides the basis for the organization and selection of standards and guidance. The relationship of this chapter to the rest of the document is shown in Figure 2-1.

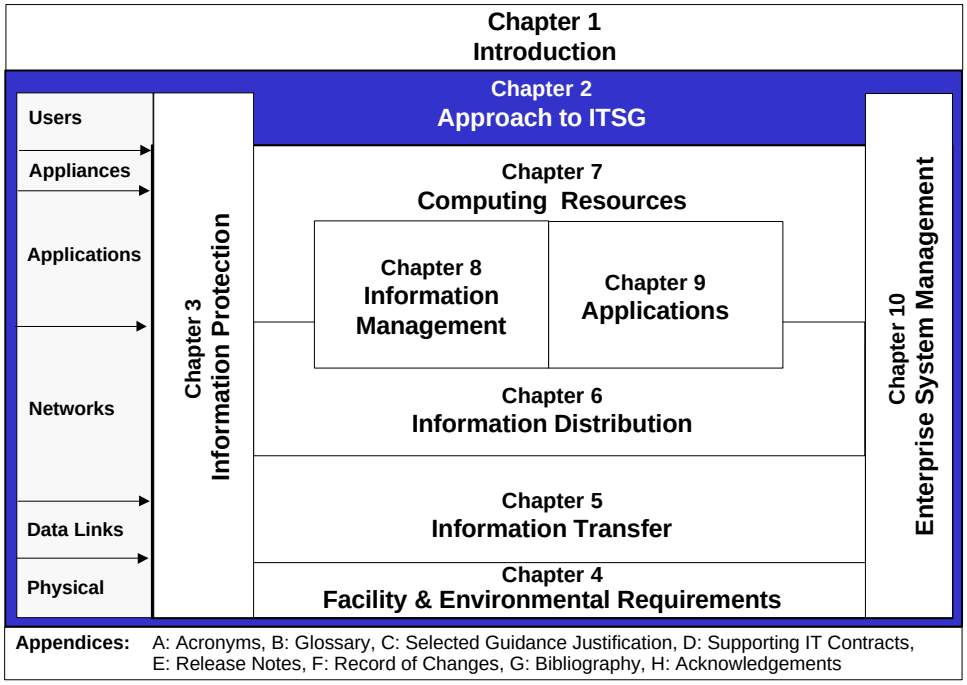


Figure 2-1. ITSG Document Map Highlighting Chapter 2, Approach to ITSG

The ITSG supports the Department of the Navy's migration from independent, application-based, stand-alone functional systems to a single enterprise information infrastructure – one that enables functional applications to be inserted and extracted as modules without disruption to the overall enterprise system. Equally important, it provides guidance to support refreshment of technology components that comprise the infrastructure itself. The ITSG is the guidebook for network-centric implementation to achieve information superiority.

The ITSG is not intended to be a shopping list of universally accepted standards that justify selections already made by program managers and system implementers, nor is it intended to be a restatement of existing documents such as the Joint Technical Architecture (JTA). It is intended to bound the options that systems implementers have so that they converge upon a common architecture and interoperability. The ITSG does provide enough tolerance, however, to allow introduction of emerging standards and selection of standards applicable to unique operational environments.

The ITSG attempts to completely cover all aspects of IT implementation and is organized so that the system developer, integrator and manager can quickly get to the information relevant to their mission. This is a challenging task because the universe of IT is vast, expanding, and moving. This chapter provides a description of the ITSG approach, organization and coverage.

The Navy and Marine Corps face the challenge of providing technologically advanced IT capabilities to the warrior and support forces while balancing these against the immaturity and uncertain market-acceptance of these same technologies. This is a special concern to network

designers as infrastructure costs are high and disruption/downtime during installation can be significant. To provide guidance to managers, integrators and designers, the goals of these standards are as follows:

- Promote national and international consensus from such bodies as the Internet Engineering Task Force (IETF), the ATM Forum, the American National Standards Institute (ANSI), the International Telecommunications Union (ITU) and others.
- Reduce the dependence on proprietary solutions.
- Offer the best potential for scalability, adaptability and market acceptance while minimizing the financial and loss-of-service consequences of choosing/replacing non-optimal components.
- Allow for controlled growth and upgrades as requirements change and expand.

2.1 Best Practices, Standards, Products and Guidance

Open system standards are embraced as the desired tenets for building the information infrastructure. Where such standards do not exist, the Department of the Navy (DON) ITSG will provide best practices or direction, if possible. When the state of the technology is not clear, the ITSG will provide as much guidance to the user as possible. Unlike the JTA and other standards documents, the ITSG is more of a guidance document so that the “strictness” of the definition of a standard does not interfere with its usefulness and timeliness in supporting the architecture. Simplified definitions of these guiding elements are provided below and are intended to put useful guiding principles, not limited to standards, in context. They offer perspective on how a guiding element applies to Information Technology (IT) development, integration, acquisition or operational implementation. The formal definition of these terms is provided in the glossary, Appendix B.

Policy. A standing set of general principles or guidelines on a topic deemed to be mandatory.

Guidance. Any statement of direction or recommendation, not necessarily mandatory.

Specification. A well defined, well described design, protocol, or practice.

Standard. A selected and approved specification or set of specifications by an authoritative body.

De facto standard. A specification or product that by its sheer market acceptance is considered to be the most suitable.

Best Practices. Practices that are considered to be the most effective and efficient.

Available Products. Products that meet the system requirement.

Preferred Products. Products that are deemed more suitable than others.

2.1.1 Open System Standards

An open system describes products and technologies that have been designed and implemented according to open interfaces. Interfaces are considered open if their specifications are readily available to all suppliers, service providers, and users, on a non-discriminatory basis. They are

revised only with timely notice and public process. The DON CIO also recognizes that openness is not truly achieved until multiple commercial companies adopt and implement those standards.

Several organizations have developed and continue to maintain standards for open systems. The DON ITSG Integrated Product Team (IPT) has examined the standards of these organizations while considering the joint requirements of the DOD, services (Navy, Marine Corps, Army, and Air Force), and other agencies. In order of preference for the standards presented, these organizations are as follows:

United States standards bodies – These organizations include American National Standards Institute (ANSI) and the National Institute for Standards and Technology (NIST).

International standards bodies – These standards organizations develop and maintain international standards:

International Organization for Standardization (also known as International Standards Organization [ISO]) – This body issues standards on numerous subjects ranging from hardware and software to information processing. ISO consists of the national standards organizations of more than 89 member nations.

International Telecommunications Union-Telecommunications Standardization Sector (ITU-T) (formerly named Consultative Committee on International Telephony and Telegraphy [CCITT]) – This body, responsible for worldwide telecommunications standards, makes technical recommendations about telephone, telegraph, and data communication interfaces. ITU-T is part of the United Nations treaty organization called International Telecommunications Union (ITU). ISO and ITU-T sometimes cooperate on issues of telecommunications standards. ISO is a member of ITU-T.

Internet Engineering Task Force (IETF) – The IETF, under the responsibility of the Internet Activities Board (IAB), publishes Requests for Comments (RFCs). The body of RFCs comprises a widely implemented set of Internet protocol suite standards. These standards are the basis for the strategic interconnection technologies of the public Internet

Institute of Electrical and Electronics Engineers (IEEE) – The IEEE sets standards for various communications and systems interfaces. IEEE defined Portable Operating System for Information Exchange (POSIX) standards that the U.S. government has adopted.

Industry Consortia – These consortia consist of end users, software suppliers, and computer manufacturers, and are international in scope and influence. Industry consortia considered in the DON ITSG include: The Open Group (TOG), which was created through the merger of X/Open and the Open Software Foundation (OSF), the Network Management Foundation (NMF), and the Asynchronous Transfer Mode (ATM) Forum, among others.

National standards bodies – It may be useful to follow standards from organizations. These organizations include British Standards Institution (BSI), French Association for Standardization (or Association Française de Normalisation [AFNOR]), German Industrial Standards Institute (or Deutsches Institut fur Normung [DIN]), and Japanese Industrial Standards Committee (JISC).

2.1.2 De Facto Standards

Even though open systems standards are embraced as the desired goal for the DON, de facto standards cannot be ignored and must be incorporated to some degree. Increasingly, de facto standards are becoming the industry determinant for technology evolution because the open systems process, by its very nature, will never move forward as rapidly as the de facto standards process. In some cases, de facto standards may be preferred over open standards that are not complete or not widely supported by available products. Additionally, de facto standards must be adopted because of wide use or acceptance. The ITSG IPT will incorporate prevalent de facto and industry consortia standards as appropriate.

2.1.3 Product Suite and Products

Where there is no standard, the ITSG will provide as much guidance as possible on the selection of product suites or products. Product suites or products will be embraced when current standards are insufficient to guarantee interoperability.

Information service providers must develop and integrate platform architectures using products from multiple suppliers. In many IT areas, competing standards and products provide little basis for selection. Here, the concept of working sets, or product suites, has gained popularity. Users can choose a collection of products and capabilities that promise to work well together to minimize the risk of incompatibilities among multiple-vendor products that are not built to work together. The cumulative advantages of a suite of products often outweighs the competitive advantages from using “open” products that have their unique “features”. The ITSG recognizes this and seeks to take advantage of these working set efficiencies

2.1.4 Order of Precedence

All things being equal, products that comply with open system standards are the preferred choice. Products that support de facto standards are the second choice. However, to perform a common function, the Navy and Marine Corps will not accept multiple, non-interoperable products. A single product suite or single product that tightly integrates multiple functions well is preferred over a federation of products, assuming there is an associated improvement in performance or price and guaranteed compliance with future open system management standards.

2.2 Application of Standards and Guidance

The specific use of standards and guidance varies depending upon the role of the IM/IT worker. A software engineer normally thinks of elements within a programming toolkit such as the Distributed Computing Environment (DCE). The system integrator thinks of interface standards such as Asynchronous Transfer Mode (ATM). The system user thinks of standard products such as Netscape. To organize these guiding elements, the ITSG places standards and guidance into three categories.

Development. How to program, design or develop a system component. Applicable to design engineers and software developers. Normally supports information processing.

System Integration. How to integrate system components into a system or system architecture. Applicable to system engineers and system architects. Supports end-to-end information flow.

Operational. What to use and/or how to configure and implement a system to maximize operational effectiveness. Applicable to process improvement. These are required for business and warfare process improvement.

2.3 Level of Abstraction

Like the application of standards and guidance, the associated level of detail also spans a range of needs. For example, the specific details of the International Telecommunications Union – Telecommunications (ITU-T) X.400 standard for electronic messaging is important to the developer of an electronic mail (e-mail) application. On a higher level of abstraction, the system engineer tracks the interface specifications of the standard to understand the compatibility between products as well as interoperability and translation requirements with other standards. The system engineer also understands other standards such as the Internet Engineering Task Force (IETF) Simple Mail Transfer Protocol (SMTP) standard and needs to select one standard over another to maximize system integration. At the greatest level of abstraction, the project manager understands the rationale for the selection of a particular standard such as SMTP over X.400 to guide system development and to identify products that support the messaging capability.

The three levels of abstraction are:

Technical. Highly precise and very detailed set of specifications that describe a standard or practice.

Integration. A more generalized description of standards — practices that reference technical specifications with specific application guidance.

Management. A description of the information system characteristics provided by a set of referenced standards or guidance and how it translates into total architecture capability.

The ITSG aims for the middle level of abstraction – integration, recognizing that a greater level of technical detail may be needed to ensure interoperability. Comprehensive coverage of the technical level would require significant documentation that would restate information already maintained by competent technical authority. Included in the integration level will be references to the technical specifics of a particular standard, specification or guidance to allow the reader to obtain greater detail. The integration level addresses each information technology category with an overview that discusses the standards and guidance selected with the associated rationale. A future ITSG document or web page will include a management summary that links the technology summaries for a single source at the management level of abstraction. For this first product, however, the focus of the ITSG is on system integration to improve the operational performance of the information infrastructure.

2.4 System Capability

The four core system capabilities listed below provide the foundation for functional (e.g., logistics, administration, C4ISR, operations) applications. A system architecture, technical standards and guidance will support the development and sustainment of these capabilities across the Naval enterprise. Each of these capabilities is created by a collection of platform/activity systems interconnected and integrated, thereby providing a full enterprise capability. Each system

is determined by considering the platform or activity mission and operating environment. The four core system capabilities are:

Local Area Network (LAN) and Core Client Services. This includes a backbone, hubs and tail segments to devices. The devices include, at a minimum: primary and secondary domain control servers and PC clients for command identified users. Core client services include those required by commands to effect business and operational process improvement across the Naval enterprise.

Dispersed Communication for Deployed Forces. Ships and deployed Marine Corps elements require robust reliable communications into the Defense Information Systems Network (DISN) normally via Satellite Communications (SATCOM) for C4ISR and Tactical Support.

Wide Area Communications for Shore and Garrison Forces. Shore commands and Marine Corps garrisons need connectivity to the DISN to reach deployed forces and other supporting units.

Basic Network and Information Distribution Services (BNIDS). These are the very basic network services and the most fundamental applications that all platforms and activities need independent of their command mission and operating environment. BNIDS include network packet or circuit delivery, domain name service, directory service, electronic mail (e-mail), web service, file storage and transfer, network time service and network news service. (Chapter 6, Information Distribution, contains the full list of BNIDS.)

2.5 Standards, Architectures and Infrastructure

Standards and guidance provide the fundamental elements necessary to allow the components of the architecture to be interoperable. Certification that an infrastructure is built to standards provides the credibility and trust needed by users for safe and reliable operation. Information technology standards and guidance within the Department of the Navy are needed to achieve secure, credible, and comprehensive support of operations and business practices. The metaphor used in the JTA describes standards as the “building code”. Unlike a building infrastructure, which is totally grounded in physical principles, the information infrastructure must become the established discipline and order in a logical environment as well. To build this infrastructure, architecture is needed that supports both the logical and physical environment. Additionally, the architecture needs to be responsive to information technology advancements to ensure infrastructure evolution with attendant improvement in operational practices, ease of use, and minimal disruption.

2.5.1 Supporting Infrastructure Evolution

2.5.1.1 Transitioning the Naval Information Infrastructure

The advancement of network communication technology offers opportunities for greater efficiencies and economies of scale by combining electronic information flow onto a single logical network service. In the past, transport of information on specific physical media drove the technology and associated system management structure. Typically, a separate support and management structure was required for telephone, computer and television/video

teleconferencing systems. We now have the capability to combine voice, video and data transmission onto the same communication network. Figure 2-2 illustrates.

As shown in Figure 2-2, voice, video and data applications currently require separate infrastructures for each information type. Better efficiency, economy of scale, and interoperability are attained by combining all information onto a single integrated network. Edge devices can be provisioned to interface two specific media types.

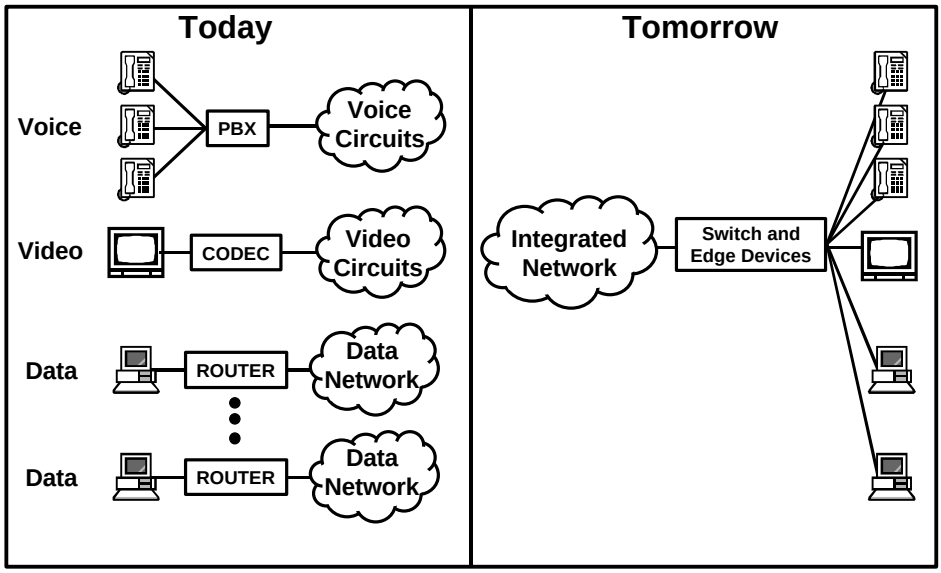


Figure 2-2. Transition of Information Technology

2.5.1.1.1 Factors Affecting Transition

These factors support the consolidation of the information infrastructure:

Economics. The ability to attain better information processing and dissemination capability. The potential for improved economics provides impetus for consolidation of information onto a single infrastructure.

Interoperability. Previously, information transfer and storage decisions were determined based on the physical media used for transport. The ability to mix and match information from video, voice, print and computing was not possible because the protocols and the physical transport media were not interoperable. Digital electronics, advances in protocols, and the technology to support a wide range of transfer rates has removed that limitation. Now, we can combine voice, video, and data on common information systems for improved system interoperability.

These factors support the separation of the information infrastructure:

Security. Until recently, incompatible physical media provided natural separation barriers that mapped to natural security boundaries. As we transition to common protocols and media, new technology and organizational discipline must provide secure separation of information.

Organization and Management. Similar to security, physical media incompatibilities provided a natural scope to the span of control managed by the information system manager. Systems were created based on the media types and entire management support structures were created to manage end-to-end information flow within the media limitation. These system management structures, however, often impede new efficiencies available using common media. Organization and management influences maintain some division of information span of control, but not necessarily those implemented by legacy system management structures.

Economics and interoperability are the basis for consolidation of information technology assets. On the other hand, security and management are the basis for maintaining the separation of these assets. The drivers for these are often in direct conflict with one another, e.g., consolidation may provide economies but can negatively impact responsiveness to diverse customer requirements or integrity of security enclaves. The ITSG seeks to achieve a balance between consolidation of multiple technologies and separation of information technology functions by optimizing all relevant drivers.

2.5.2 Characterizing Information Technology

2.5.2.1 Redefining the Infrastructure

Information technology now offers the capability to provide a single ubiquitous network supporting all information including voice, video and data. To exploit this capability, the DON ITSG IPT has identified the following top-level categories of the Information Infrastructure:

System. The information and data processing resources, associated peripheral devices, supported applications, and the communications network infrastructure that interconnects the end users and components of the system. Systems include hosts, operating systems, peripherals and system applications, databases, and files. A system also includes all hardware and software components, facilities, personnel, and procedures that are necessary to support applications.

Network. The set of switching and transmission subsystem communication components to support information transfer. The network includes all hardware and software communication components residing in switching, routing, and transmission subsystem components, as well as communication-related hardware and software and those components that reside in hosts (e.g., communication protocols). The network also includes the organization and configuration of embedded hardware and software to support orderly and logical information distribution.

Application. A collection of system components that supports a particular task or function. It includes end-to-end, multi-media communications as well as information management and decision support capability. Distributed computing applications are normally built using a three-tiered architecture consisting of the application server, data server, and presentation clients which may be physically on a single device or on multiple devices connected by a network. Communication applications normally involve a minimum of two communication devices connected by the network.

Appliance. Any device by which an end user receives, processes, or transmits information on the selected media. Information appliances include computers, telephones, televisions, video teleconferencing equipment and the like. It is also the hardware component that is part

of an information appliance suite such as a mouse, keyboard, or video screen. In the three-tiered application architecture, these devices are referred to as “presentation clients”.

Information. The assembly and presentation of data in a form that is understandable and valuable for conveying knowledge and making decisions. It is the “payload” of the information infrastructure.

The network forms the foundation for the system, applications and appliances. Appliances are the user’s interface which connect to the network so that data and applications can be accessed. Applications are the software programs, information tools, and databases that the user operates to perform tasks. Applications transcend the network and the appliances. They involve multiple distributed computers and databases including the data server, application server and presentation client software. Application management includes coordination of the network managers and appliance managers so that the program software can access the data and processors needed.

Figure 2-3 and Figure 2-4 respectively provide illustrations of the operator’s perspective and the system manager’s perspective of these system infrastructure categories.

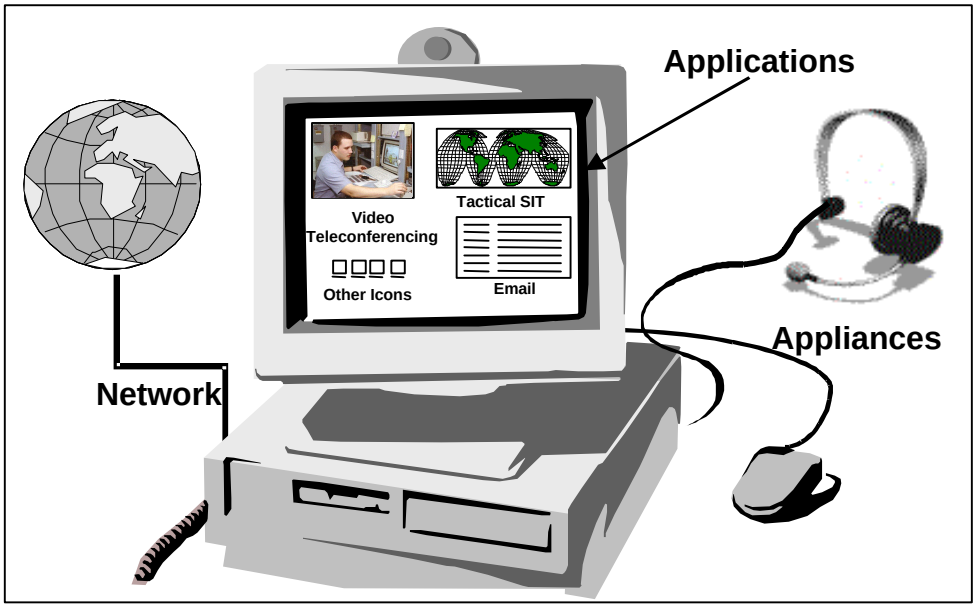


Figure 2-3. Operator’s Perspective of the Information Infrastructure

The operator interfaces with the computer, video equipment, headset or telephone and cares about running applications, getting and transmitting information independent of the physical location of the information.

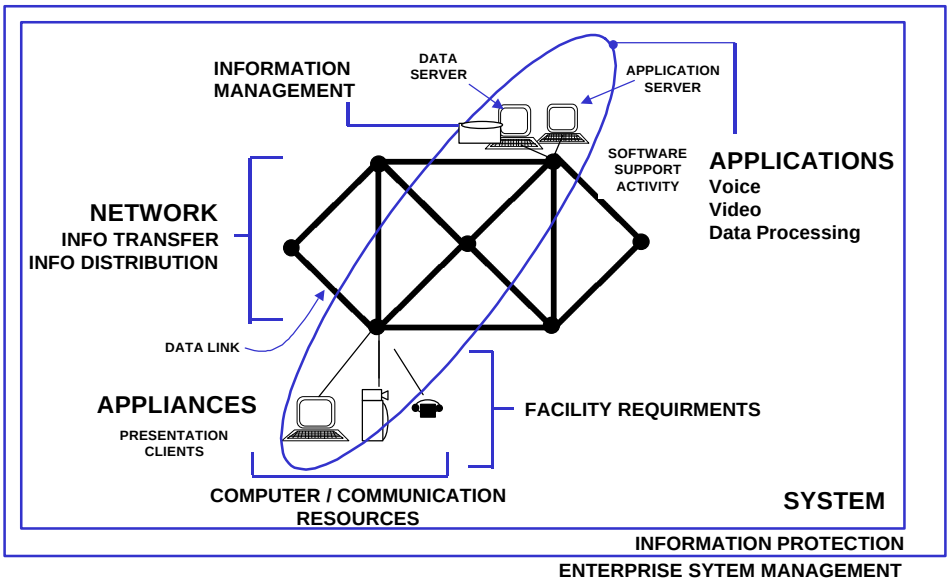


Figure 2-4.System Manager's Perspective of the Information Infrastructure

The system manager cares about appliances, network nodes, links and associated equipment. He also cares about interoperability of the software across the network, with the appliances, various databases and software management facilities that support the end user's application.

2.5.2.2 Information Technology Categories

The simplicity of system, network, appliances, applications, and data is good for the management level of abstraction, however, the system integrator needs greater fidelity. At the system level there are foundation principles that must be considered when implementing any system component. Security and physical requirements (e.g., power) must be met. Additionally, after implementing the system, the entire system must be managed and system quality must be assessed through the use of metrics. Within the network category are components that must be considered in both the physical and logical environments. These can be categorized as "information transfer" for the physical network and "information distribution" for the logical network. The quality and format of the information itself must be considered for use by the applications for processing and presentation. Using the previously defined single ubiquitous network as the model, voice and video systems are considered as applications of the system and are assigned to the applications category. The ITSG provides a level of organized segmentation to the system integrator by arranging and presenting information technology standards and guidance in eight categories. These categories are shown in Figure 2-5 as they relate to the system manager's view (Figure 2-4). The stack shown on the left of Figure 2-5 resembles the seven layer Open Systems Interconnect (OSI) model. The OSI model, however, only applies to internetworking. ITSG information technology categories transcend the network and support total information system implementation to maximize operational capability.

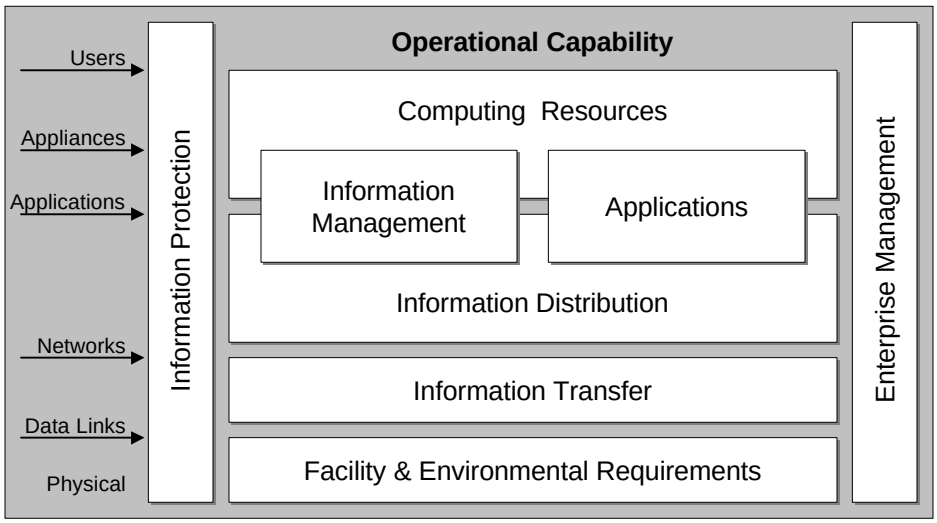


Figure 2-5. ITSG Information Technology Categories

The development of ITSG information technology categories are used to support the transition from an application-based system implementation to an infrastructure-based system implementation. This organization supports convergence to a single ubiquitous network for all applications and information media while continuing to allow for separate networks necessary for security separation and differences in technology maturity.

These categories are intended to organize standards and guidance into groups that focus on each layer of the architecture. Taken together, standards and guidance used from all of these categories will provide comprehensive support of the enterprise infrastructure. The order of the categories is important. In the selection of standards and guidance, certain fundamental security and physical factors have to be established before other standards can be selected. Information Protection is the first category and includes the security standards and guidance that other categories must follow. The Facility and Environmental Requirements category addresses the power, cooling and physical security required for the physical installation. The Information Transfer category addresses communication circuits and the physical, logical link, and network layers of the OSI model to move information across the network. The Information Distribution category addresses the most common protocols and formats needed to process and present information such as e-mail and web service. The Computing Resources category uses the Information Protection, Facility, and Transfer standards and guidance to ensure computers and peripherals are interoperable with the infrastructure and the user through Disk Operating Systems (DOS), Network Operating Systems (NOS) and the Human Computer Interface (HCI). The sixth category, Information Management, addresses the format and structure of data-at-rest so that some commonality of information in data bases and data warehouses exists for presentation, interpretation and use by applications. The seventh category, Applications, addresses the software programs and end-user system capabilities such as voice, video and collaborative tools needed by the operators to perform their mission. The eighth and final category, Enterprise Management, that addresses standards and guidance for managing the information infrastructure and metrics to measure its efficiency and effectiveness across the enterprise. These categories are the basis for each chapter of the ITSG.

2.5.3 The Logical Environment

It is difficult to think and operate in terms of a logical environment. Metaphors are created to link logical concepts with physical realities, hence the use of the term ‘virtual’. For example, the term ‘virtual reality’ labels items that appear to our senses to be actual physical entities but that are actually created through logical configuration and presentation of sensory data. Likewise, the term ‘virtual network’ refers to the logical configuration of what could be multiple physical networks interlinked into a set of networks tailored to a particular operation or business process. This logical environment, with its distributed data, is referred to as “cyberspace” in the Internet culture.

2.5.3.1 Benefits

The logical environment is free of physical constraints and has more degrees of freedom to foster innovation. For example, a worldwide virtual network allows creation of a ‘virtual office’ of individuals widely dispersed over long distances and performing as a single team. In the ITSG, virtual networks and logical networks mean the same thing.

2.5.3.2 Challenges

The multiple degrees of freedom in the logical environment make order and discipline a greater challenge. For example, physical safety is not a direct concern in the logical environment; as a consequence, very little mechanical competence is required to create (or destroy) logical infrastructures. To illustrate, compare the impacts in allowing a four-year old child to drive and crash your car versus allowing him or her to operate and trash your computer’s hard drive – the physical damage is much worse than the logical damage. Conversely, security is a monumental challenge because of the many degrees of freedom available. The ability to traverse many logical environments from a single one is trivial unless logical separation controls are implemented. A constant tension in IM/IT is how to exploit dramatic IT advancements through the logical environment while maintaining the security of critical information. This tension is characterized as security versus freedom. The information infrastructure requires a carefully administered risk management approach that considers a combination of physical and logical measures for adequate security, but enough freedom to be technologically agile and operationally responsive.

2.5.3.3 Virtual Private Networks (VPNs)

With the advent of such technologies as Asynchronous Transfer Mode (ATM), Virtual Private Networking (VPN) has become one of the fastest growing applications of advanced networking technologies. VPNs are logical extensions of physical networking technologies, e.g., physical LANs located in different geographical areas can appear to the user as a single logical LAN – even though a WAN interconnects them. With previous technologies, VPNs were limited because making use of all available bandwidth was paramount to amortize circuit costs. Multiple “bursty” streams were multiplexed via routers to produce a single stream with lower peak demands. This traditional “best effort” scheme was adequate for general data transfer, such as e-mail and file exchange. However, interactive and time/delay sensitive streams had no guarantees that physical networks would deliver information packets on time.

More demanding applications, such as interactive graphics and multimedia, require a more robust approach. A practical solution is ATM. It meets these more stringent demands by offering a more controlled Quality-of-Service (QoS) environment and an accommodation for varying traffic patterns. ATM is a key factor in creating VPNs. QoS will allow network components to multiplex

streams while meeting their latency and bandwidth requirements. With a single protocol that scales from kilobits per second to gigabits per second, and spans LANs and WANs, ATM offers a solution for a global virtual private network – an intranet that rides on shared infrastrucutre.

2.5.3.4 Logical Infrastructure Model

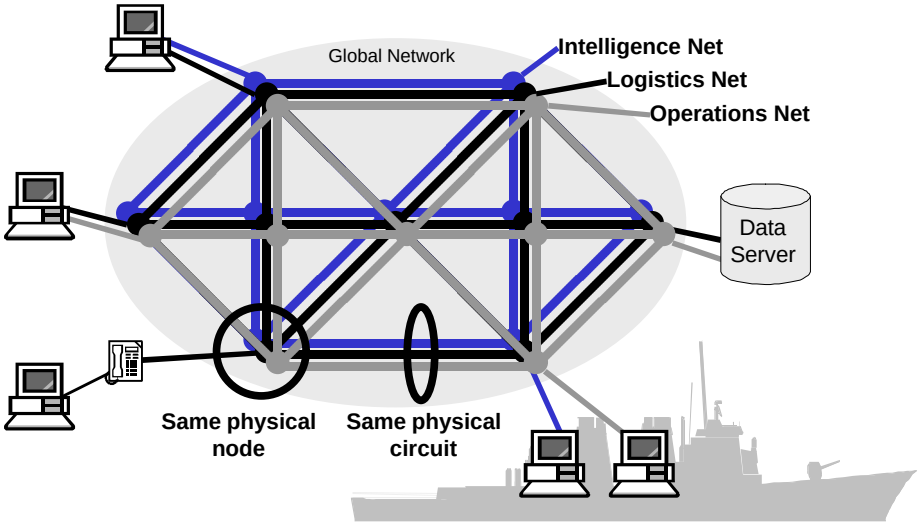


Figure 2-6. Logical Infrastructure Model

Figure 2-6 is a logical infrastructure model that shows three virtual networks supporting five notional users. All users and resources appear to the user to be on the same single network. Physically, other virtual networks share the underlying network links and nodes.

Figure 2-6 provides an example of the simple logical infrastructure model used in the ITSG. As shown, there are three worldwide virtual networks supporting intelligence, logistics and operations, both afloat and ashore, for tactical and tactical-support operations. These networks could represent a network supporting a particular project, releasable information and accessibility to selected foreign nationals, or any other mission area information domain. The underlying physical infrastructure is transparent to the users of the network. All users have access to multiple virtual networks and an information server that supports multiple virtual networks. From a security standpoint, information can flow on common circuits though common, redundant switches and routers. However, at each node, additional protection, encryption and filtering is performed to ensure that only the community of interest can access workstations, processing centers, and information sources. Special measures are taken at the physical network interface nodes to protect against outside or public intrusion.

2.5.4 Area Network Designations

2.5.4.1 Background

As computer networks evolved, different technologies were best suited for the different distances covered. Local Area Networks (LANs) consisted of a network media shared by numerous computers and peripherals under a single management control. Wide Area Networks (WANs) consisted of point-to-point links that connected LANs together using routers, gateways or bridges. Metropolitan Area Networks (MANs) were contrived as small WANs – point-to-point links that connected a relatively high concentration of LANs together within a regional area. LANs, MANs

and WANs were interconnected to maximize computer communication capability among network subscribers. The designation of a particular network as a LAN, MAN, or WAN was primarily due to the domain of circuits and nodes that was under a single management control, normally aligned with the geographic area of coverage.

2.5.4.2 Paradigm Shift

New switching technology combines the best characteristics of shared media and point-to-point network protocols. It can directly connect a multitude of end users over great distances without the traditional network gateways. Hence, the use of "geographic area" to designate a network perimeter is losing its relevance. Because the predominance of this new technology fosters physical and logical networks that transcend geography, the definitions of LANs, MANs, WANs, and related "area networks" have become ambiguous. An "area" no longer bounds the network domain; therefore a new understanding has to be adopted. All of the below descriptions are valid and at least one is relevant, depending upon the point of view of the information worker (see Figure 2-7).

Economic definition: LANs are networks that the user owns, and WANs consist of services that are purchased from an external service provider (either commercial or a corporate department significantly removed from the user). The language of the telephone industry applies – the circuit demarcation point defines the boundary.

Geographical definition: LANs historically spanned a room, ship or building while WANs crossed the country. As LAN technology expanded to network multiple buildings, the terms Metropolitan and Campus Area Networks were created. The advent of high-speed local-loop technology and end-to-end switching, as in ATM, has further blurred this definition.

Control definition: From a network manager's point of view, it is reasonable to treat the control domain as a LAN, and everything outside that domain as a WAN. This definition does not necessarily have geographic significance, but the entry/egress point between the LAN and the uplink network (e.g., the Internet) is the defining boundary.

Other factors that closely relate to the LANs and WANs definition:

Security definition: LANs traditionally stopped at the user side of a router or firewall. With Virtual Private Networks (VPN), geographically separated LANs can now be bridged into a single community of interest.

Bandwidth definition: Until recently, LANs could sustain higher orders of magnitude transfer rates than those of WANs – namely 10's and 100's of Megabits Per Second (Mbps) for LANS versus 1's and 10's of Mbps for WANs (see 5.1.3). The gap in the two rates has rapidly closed as increases in long-haul bandwidth have far outpaced increases in LANs. Because the cost per bps of bandwidth is still significantly higher with WANs, the traditional definition is still valid in many cases. Also associated with bandwidth, bit error rates in WANs can be higher, particularly in shipboard communications.

Standards definition: LANs were standardized in ANSI and IEEE while WAN components were generally standardized by ITU-T (formerly CCITT). The formally designated Metropolitan Area Network (MAN) standard (IEEE 802.6) has not seen widespread use or vendor support. Homogeneous switching fabrics, such as ATM, blur this definition. Because this is a generic definition, it is of marginal use.

The adopted convention could be characterized by the same names but not necessarily the same description. The appropriate definition of a LAN, MAN or a WAN depends on the management, application, and architecture and may change as a system expands. This document provides the standards and protocols necessary to develop various architectures, based on the design goals of the system engineer or system manager.

Characteristics	Local Area Networks (LANs)	Metropolitan Area Networks (MANs)	Wide Area Networks (WANs)	Virtual Private Networks (VPNs)
Geographic	Room, Platform, Ship, Building, Campus	Campus, Base, Town, City, Metropolitan Region. Local Loop Connects To The WAN	Region, Country, Theater, World	Not Applicable
Economic	Implemented by a program of record with appropriated funds or by the command using command budget	Services purchased from a carrier or owned and operated by a DISA or Service regional center	Services purchased from DISA or a commercial carrier	With ATM or single vendor IP routing network services, cost of tailored configuration by command budget or appropriated funds
Control	Single management within the end user command	Single or multiple management outside the end user command	Single or multiple management outside the end user command	Single or multiple management outside the end user command
Security	Safe trusted enclave behind a security firewall and encryption device.	Safe enclave consisting of interconnected enclaves all behind a single security firewall. Classified links are bulk, link or source encrypted.	Some protection of interconnected enclaves each with their own firewall. Links are normally bulk encrypted	Safe trusted enclave based upon source or link encryption of channels and trusted computer hosts and facilities within a community of interest
Bandwidth	Megabits to gigabits per second on a single channel	Kilobits to megabits per second on a single channel. May have channel aggregation.	Kilobits to Megabits per second on a single channel. Megabits to terabits per second on the aggregated trunks.	Megabits to gigabits per second per channel. Aggregate is a WAN
Standards	ANSI, IEEE 802.2 series (Ethernet) TCP/IP, ATM	IEEE 802.6 (little use). ATM, TCP/IP, PPP, ITU-T	ITU-T (CCITT), PPP, TCP/IP, ATM, Frame Relay	TCP/IP using single vendors for routers. ATM

Figure 2-7. Comparison of Area and Virtual Private Networks (VPNs)

2.5.4.2.1 System Manager View

To the system manager a network is simply the domain of circuits and nodes that fall under a single management control. There can be several network domains in a command and/or a single network domain can serve many commands over a very wide area. Geographic distance has little or no relevance to the control domain. In the ITSG, network domains will normally correspond with the Information System Domain (ISD) concept described in Section 2.5.6.

2.5.4.2.2 User View

To the end user, the concept of LANs, MANs and WANs is useful to perpetuate because it aligns the network domain with the physical or geographic domain with which we are familiar. Because of this, the ITSG will continue to refer to LANs, MANs and WANs as they relate to the end user.

2.5.4.3 Adopted Convention

The "area network" conventions adopted by the ITSG are shown in Figure 2-8.

Local Area Network (LAN). LANs use the IEEE 802, ANSI, and ATM standards — the signals travel over optical fiber cable or copper wire and all network components are under the ownership and control of the network manager. They include wireless LANs that are generally designed to support untethered network-to-end-user connections. The control definition applies here. Extended LANs include base and campus networks.

Wide Area Network (WAN). WANs are divided into two parts. The first is defined as trunk technology and switching (Telephony DS-n/T-n and Synchronous Optical Network (SONET) OC-n transport, and ATM and Frame Relay switching). For this part, the economic definition applies – the LAN provider will generally purchase these services rather than invest in wide-area equipment and cable. The second addresses what the telephone industry refers to as the "local loop," meaning the reach from the central office to the business or residence. In many cases, the customer may actually own such assets. (See Table 5-1 for a listing of DS, T and OC link designations.)

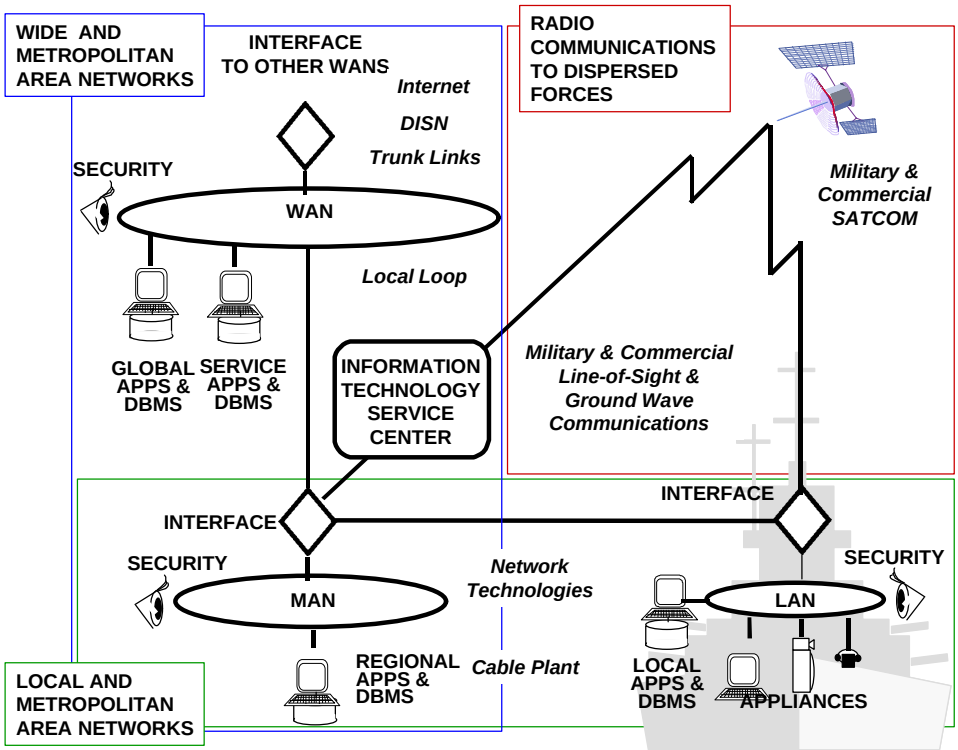


Figure 2-8. Adopted Architecture Model for LANs, MANs, WANs, and Radio Communication to Dispersed Forces

Metropolitan Area Network (MAN). MANs cover the ambiguous overlap where relatively wide area networks can take on the characteristics of a LAN or a WAN. MANs either use LAN technology extended over a "larger" regional area or use WAN technology – point-to-point links that connect a relatively high concentration of LANs together – within a "smaller" regional area.

Radio Communications to Dispersed Forces include Satellite Communications (SATCOM) and Line-of-Site (LOS) radio links to support trunk (router-to-router or switch-to-switch) connections to underway or deployed forces.

2.5.5 The Physical Environment

Figure 2-9 is an architecture model of the global infrastructure showing worldwide coverage and command echelon support from major command headquarters and global information service providers down to the tactical elements. As discussed in Section 10.5.4, the use of WANs, MANs and LANs here depicts network domains that conveniently align with geographic areas and command echelon. This is useful to illustrate multiple networks with required interfaces even though new switching technology can directly connect end users on very large networks over great distances without traditional network gateways. The model shows separate WANs, use of a worldwide fleet intranet for mobile ships, regional and base MANs for garrison and shore commands regions, LANs within the commands, and connectivity to mobile users and tactical units.

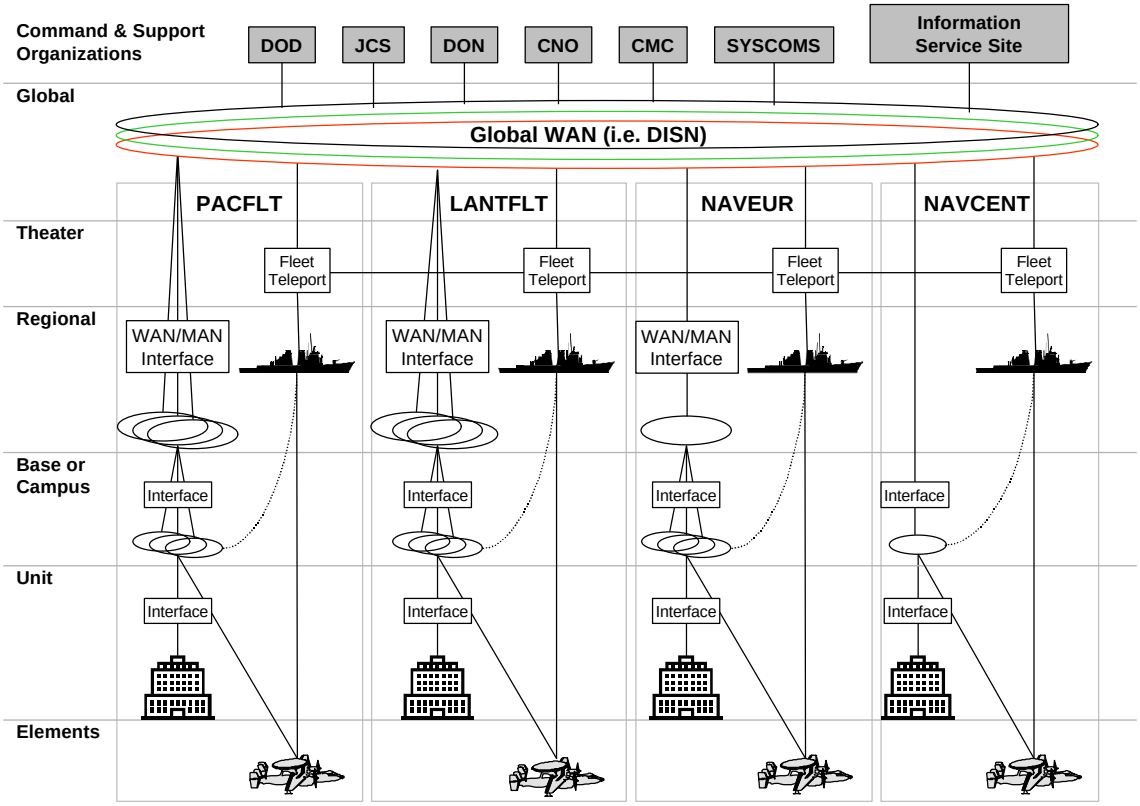


Figure 2-9. Global Infrastructure Model

Section 2.5.3 discussed the logical environment as the needed end-state to be supported by the physical infrastructure. The physical infrastructure model that supports the enterprise (represented

in Figure 2-9) shows both the geographic coverage and coverage of command echelon. Command echelon coverage is roughly the same as geographic coverage but the lower levels of the echelon focus on support of specific missions or functions. A WAN such as the Defense Information Systems Network (DISN) provides global geographic coverage. Security separation is provided by cryptographically-separated networks for Unclassified, Secret, Special Compartmented Information (SCI) as well as the Internet. Currently, the DISN is a single physical network logically separated into the Secret Internet Protocol Routing Network (SIPRNET) and the Non-Classified Internet Protocol Routing Network (NIPRNET). Units can connect directly to the global WAN but in Naval concentration areas such as Norfolk or San Diego, the global WAN / DISN is accessed via a MAN. Deployed units such as underway ships connect to the global WAN via Fleet teleports at each Commander-in-Chief (CINC) site (e.g., CINCPACFLT) and at the Commander, U.S. Naval Forces, Central (USNAVCENT). Ships are provided with seamless connectivity as they move between satellite footprints and from port to port via a Fleet intranet. This links each fleet interface to permit coordination and reconfiguration as necessary ashore to minimize configuration changes performed aboard ship and tactically deployed units. At the Naval concentration areas, shore and garrison commands are connected to base area networks. The base area networks also have connectivity to the Fleet intranet at the piers so that ships can transfer connectivity from their Satellite Communication (SATCOM) systems to pier connectivity, and vice versa, with minimum disruption of information flow. Tactical units assigned to afloat or shore commands will have communication tethers either to their parent commands or to standard network interfaces. Mobile commands or individuals on the road are also able to connect via the standard network interfaces. Information Technology Service Centers (ITSCs) will provide support to Naval components. These centers will function as a single, integrated entity.

2.5.6 Information System Domains

To achieve full integration, the architecture model is further defined to identify zones of the global infrastructure that can operate with relative independence from the remainder of the architecture. Normally, the zones are the area networks such as the LANs, MANs and WANs and the routers or gateways are the interface. These zones are designated as “Information System Domains,” (ISDs) (Figure 2-10) which include a set of clients, servers, multi-media equipment, associated peripherals and network components interconnected and bounded by interfaces to external networks or communication circuits. The ISD is managed and operated by a single organization. The information system domain concept provides the freedom to allow changes in zones of the infrastructure with minimum impact on the enterprise. The following provides additional advantages of the information system domain approach.

- Recognizes that different platforms have different operational missions and must operate in different environments (e.g., latency requirements for targeting data on a Cruiser versus delivery of orders for a Personnel Support Detachment (PSD)).
- Tolerates a “system flux” across the entire infrastructure. Allows for technology refreshment with less coordination. Different versions can be allowed as long as contained within the ISD
- Allows for some command autonomy
- Allows for a modular approach to standards implementation
- Allows exploiting new technology in controlled domains

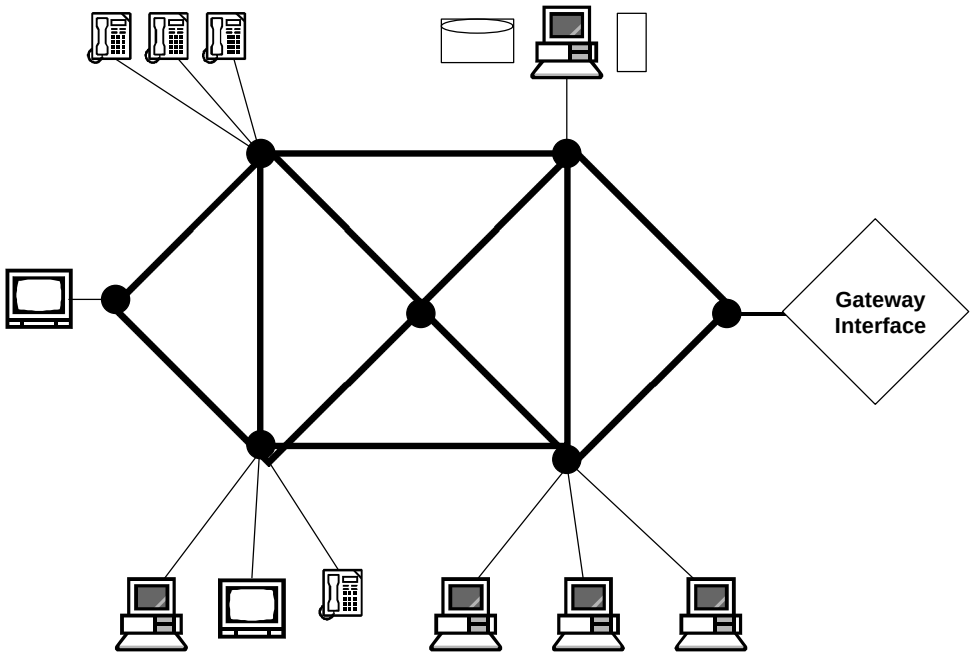


Figure 2-10. Information System Domain

2.5.7 System Domain Components and Linkages

Information system domains provide tolerance for information technology differences caused by budget and operational constraints. Critical to the establishment and sustainment of a single enterprise-wide system infrastructure is control of the interfaces between the Information System Domains. Normally, the information system domains will be a geographic area network such as a local, metropolitan, or wide area network. Each domain will have a number of interfaces consisting of devices such as routers, switches, firewalls, proxy servers, and encryption devices. These interfaces must use common standards and be strictly configured to achieve enterprise system component interoperability and integration. Figure 2-10 is a lower level view of the architecture model depicted in Figure 2-9. Figure 2-11 shows each area network from the command's LAN through the regional MAN (which can also represent the Fleet intranet). The MAN is shown connected to a WAN via an interface that in turn is connected to another WAN via an interface. Many Information System Domains will have information and application servers that can support the entire enterprise or the local region and all have to implement consistent security measures to protect the enterprise. Selection of standards and guidance is based upon using Figure 2-11 to support enterprise integration and the logical infrastructure model depicted in Figure 2-6 to support functional area networks that transcend geographic locations.

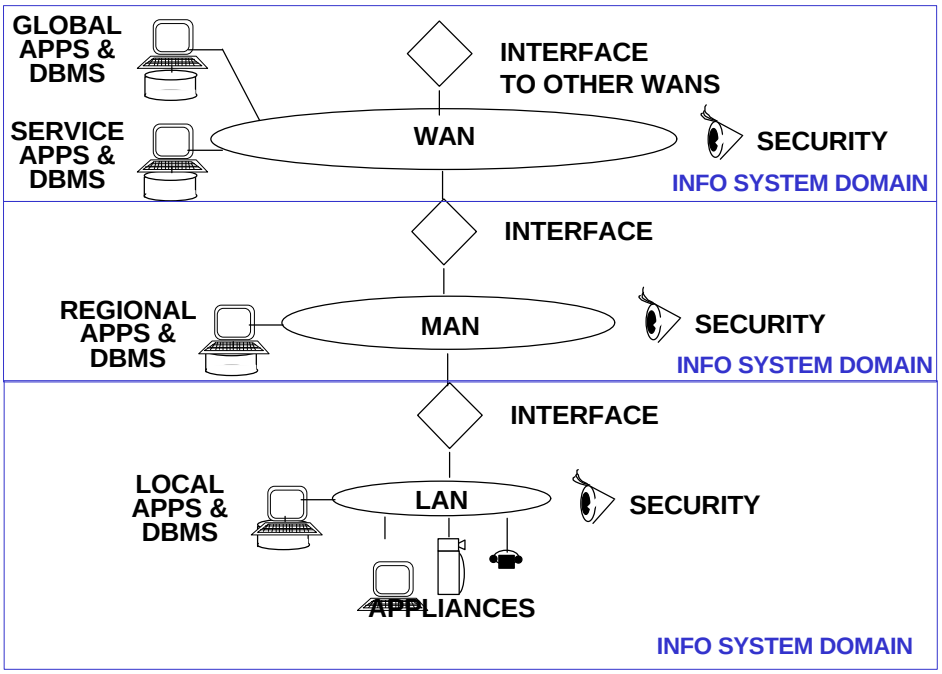


Figure 2-11. System Domain Components and Linkages

2.6 Platforms, Activities and Operating Environments

Discussed in Section 2.4 were the core capabilities that individual systems, implemented on a combination of platforms and activities, could provide for the enterprise. In the Naval environment, it is unrealistic to expect all platforms and activities to use a "one size fits all" set of standards. The specific selection of standards depends upon the platform or activity being considered. The intensity of the command mission and the characteristics of the operating environment drive the specifications called for to implement information systems. Consider the mission and operating environment of an aircraft carrier versus a Personnel Support Detachment – the command mission and operating environments are vastly different and require separate standards profiles, particularly for the external interface. To provide standards profiles that support required information flow across the Naval enterprise, categories of platforms and activities are defined. These platform/activity categories and subcategories tailor standards and guidance to meet the command mission within the operating environment of each platform.

Ships. The ITSG provides guidance specific to shipboard tactical and non-tactical systems and supporting communications. The unique performance requirements (e.g., survivability, vulnerability, latency, etc.) were judged to require specific focus on the standards and guidance relevant to nine sub-categories of ships. The nine include:

- Command Ships (LCC, AGF)
- Carriers (CVN, CV)
- Missile Shooters (CG, DDG, FFG)
- Submarines (SSN, SSBN)

- Other Combatants (DD, FF, PC)
- Large Amphibs (LHA, LHD)
- Small Amphibs (LPD, LSD, LST)
- Logistics (AO, AOE, AS, AG, AE, ARS)
- Auxiliaries(AGSS, MCM, MCS. MHC)

Information Technology Service Centers (ITSCs). The ITSC is proposed as a nexus of engineers, technicians, and administrators that use system management tools to provide comprehensive IM/IT support to the Naval information infrastructure. The ITSC provides information system operation, implementation support, and administration for a community of information producers and consumers. The ITSCs should be "Local Control Centers" in full compliance with the Joint DII Control Centers Concept of Operations (CONOPS). Each ITSC would perform three major duties:

- Provide integrated information system implementation, control and maintenance
- Interface information flow from network to network including dial-in service
- Provide consolidated information and application servers, and serve as the distribution center for individual commands in the region

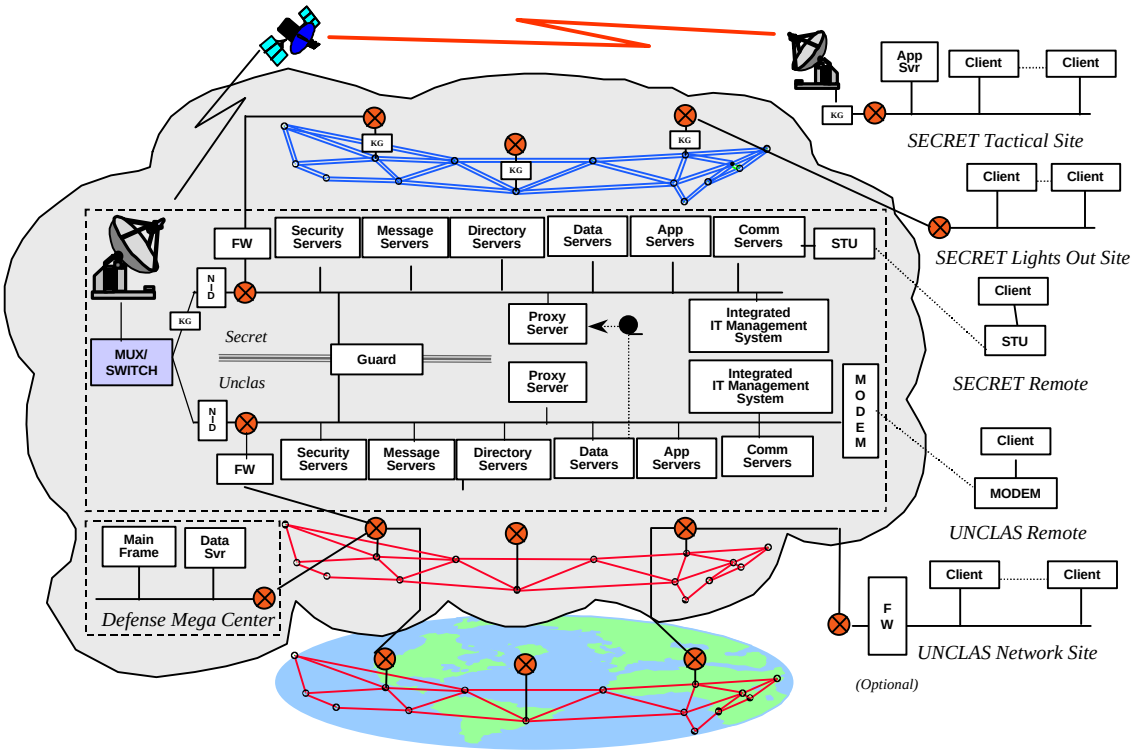


Figure 2-12. Information Technology Service Center

In Figure 2-12, the contents of an ITSC is shown within the dashed box including information servers, application servers and an integrated IT management system. ITSCs are

distinguished from shore commands by their critical infrastructure support and interface. They also provide a “pivot” to minimize disruption in service for ships that come into port and staffs that embark. ITSCs are discussed in more detail in Chapter 10.

Garrison/Shore Commands. The shore-based garrisons and commands have a wide range of tactical and non-tactical operations and support requirements. Peculiar requirements specific to location, mission, media, and other criteria require that the following sub-categories of these environments can be specifically addressed.

- CINC Joint
- CINC Fleet
- CDR Type
- CDR Force
- CDR Region
- CDR Group/Squadron
- Base-Station
- Air Wing/Squadron
- Group-Squadron
- Marine Garrison
- Medical/Dental Facility
- Training Facility
- Maintenance Facilities - Air Rework Facilities and Shipyards
- Technical Support – Laboratories, System Centers and Engineering Centers
- Personnel Support Activity (PSA)- Personnel Support Detachment (PSD)
- Small Craft Support
- Construction Battalion (CB) Facility
- Explosive Ordinance Disposal (EOD) Facility
- Supply Facilities - Depots and Weapon Stations
- Miscellaneous Facility - Naval presence at Contractor sites

Embarkables. This operational environment considers a command that must routinely move between shipboard and shore environments. The emphases for embarkables shall be on portability and “snap-in” connectivity in the corresponding ship, shore, air, ground and ITSC environments. The following types of commands can be considered embarkable.

- CDR Numbered Fleet
- CDR Group/Squadron
- Air Wing/Squadron
- Embarked Support Staff
- Embarked Marine Expeditionary Unit (MEU)

Ground. This combat-focused environment has very unique and demanding information technology requirements. This category will primarily focus on the Marine Corps and mobile command centers such as a Mobile Ashore Support Terminal (MAST).

Air. This includes the system components in the airborne communications operating environment. This will expand over time to include connectivity across different airborne platforms.

Space. This is an emerging operational environment that must have standards specific to this mission. This category will evolve over time.

To assemble a profile of standards and guidance that will provide the four core capabilities (Section 2.4) across the Naval enterprise, all information technologies must be applied against each platform and activity mission and operating environment. Figure 2-13 provides a matrix that depicts the specific information technologies that are appropriate to the particular operating environments. This matrix provides a framework for profiles of standards and guidance in each information technology category (the column of the matrix) with a focus on enterprise integration. With all the columns complete, a row would represent a guidance profile that addresses the operating environment and mission of a specific platform or activity. In the initial ITSG, the focus is on technology-based profiles for the enterprise. Subsequent updates to the ITSG will evolve to accommodate both technology-based and activity/platform-based standards profiles.

OPERATING ENVIRONMENT & PLATFORM CATEGORY	INFORMATION TECHNOLOGY CATEGORIES							
	Information Protection	Facility & Envir. Requirements	Information Transfer	Information Distribution	Computing Resources	Information Management	Applications	Enterprise System Mgt
Shipboard Environment Command Ships Carriers Missile Shooters Submarines Other Combatants Large Amphibs Small Amphibs Auxiliaries Logistics								
Info Technology Service Centers								
Shore Environment CINCs & CDRs Base-Station Group-Squadron Marine Garrison Air Wing/Squad Medical/Dental Facility Training Facility Maintenance Facility Tech Support - Lab PSA-PSD Small Craft Support CB Facility EOD Facility Supply Facility Misc Facility								
Embarkable Environment								
Ground Environment								
Air Environment								
Space Environment								

Figure 2-13. Operating Environment Matrix

2.7 Currency of Standards and Guidance

Rapid evolutionary advances in information technology are expected to continue unabated – with resultant continued short technology life spans. These life cycle patterns can be represented and explained by “S” curves. Associated with the “S” curve is the “cost trough” that reflects an area of lowest cost as impacted by competition and availability of the technology. The “S” curve enters this trough when the technology usefulness and acceptance emerge and benefits begin to rise. The cost trough continues until saturation or maximum capability is reached and remains until rendered less beneficial by emerging/new technology. Likewise, the cost curve starts to rise as more support and alterations are required to interface the aging technology with new

technology. “S” curves can also be used to track and anticipate innovation cycles. Overlapping “S” curves within a technology domain often show where the benefits of one innovation peak and decline, while the next innovation gains acceptance and accelerates. By comparing specific technologies with other important technologies in the industry, organizations can better anticipate and plan.

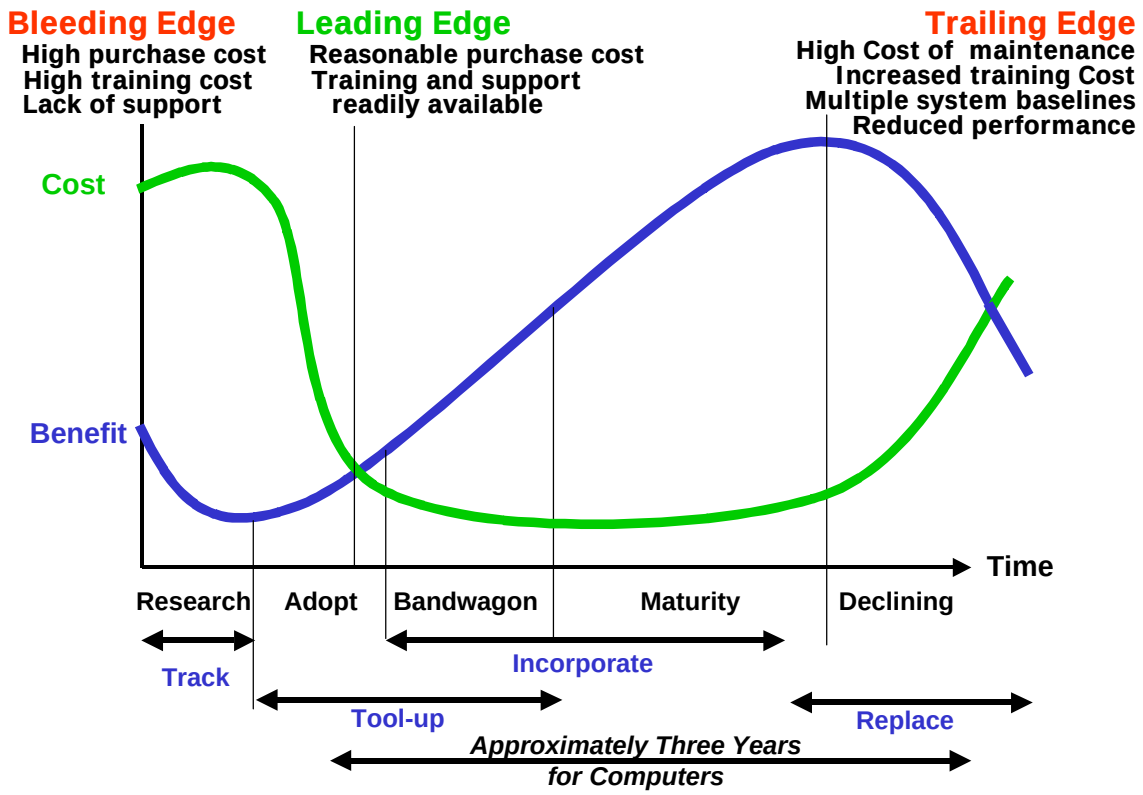


Figure 2-14. Technology Life Span

Shown in Figure 2-14 is the benefit “S” curve that starts low but peaks as the technology matures. Likewise the “cost trough” goes from high at the “bleeding edge” of the technology, bottoms as the technology matures, then increases as the technology becomes less popular and is more difficult to support. The pace of IT innovations has increasingly shortened the life spans of IT products. The technical complexity of products is also increasing. The high mobility of forces and rotation of support personnel make this product turnover and complexity especially acute for the Navy and Marine Corps. Figure 2-15 depicts a recommended ITSG implementation structure for a specific technology life span. This table will be used throughout the ITSG to provide guidance to commands to plan and budget for required infrastructure changes. DON IM/IT strategy will change at a reasonable rate – one that keeps us current but minimizes changeover disruption. Use of the Information System Domain concept (in Section 2.5.6) will allow for incremental change across the Naval enterprise while maintaining enterprise-wide interoperability.

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Selecting any of these specifications, products, or technologies is not recommended.	Select specifications, products, or technologies based on this time line.				These specifications, products, or technologies are being monitored as potentially significant.
Activities, Platforms, Operational Environments	The specifications, products or technologies above apply to these platforms or operational environments.				

Figure 2-15. Sample ITSG Implementation Time Line

- The Not Recommended column specifically identifies certain technologies, specifications or products that significantly deviate from the preferred direction due to lack of interoperability, security, supportability, etc. The information system implementer should avoid selecting technologies or products listed in this column.
- The dated columns provide a time reference for choosing and aligning with DON technology direction. The standards and products listed in these columns constitute the guidance for the years depicted.
- The Emerging column highlights specifications or guidance that are potentially significant but are not convincing enough to appear on the time line of current ITSG. DON activities are monitoring these specifications and guidance for development maturity.
- The order in which entries are listed within a column has no significance.

2.8 Degree of Compliance

The last element in the ITSG approach is the degree of compliance required. There are clear advantages to making all elements of the ITSG mandatory. However, the dynamic nature of information technology, its different applicability to each operating environment and mission, and necessity to rapidly integrate emerging technology dictate the need for some latitude in compliance. To give the IT system implementer or manager comprehensive guidance on the strength of the need for compliance, three degrees of compliance will be associated with each ITSG:

Mandatory. These items must be followed under the conditions indicated without deviation. This original release of the ITSG contains no mandatory guidance.

Recommended. These items should be followed under the conditions indicated but deviation is allowed to account for special circumstances determined by on-site system managers or system developers.

Proposed. There is no requirement to follow this item. It is provided to allow advance planning. This would be associated with an emerging specification or guidance.

2.9 Standards and Guidance Selection Criteria

The DON CIO has established a standards selection criteria to be used in developing the DON IT Standards Guidance. The specific guidance given in selecting standards is that they should meet

the following criteria: (1) security, (2) functionality, (3) interoperability, (4) performance, and (5) business issues.

Security. Information protection involves both system security and information security. Selected standards must support the ability to provide both system and information security.

Functionality. Standards and guidance must support the fundamental requirement to ensure that IM/IT systems effectively and efficiently support the operational mission/requirements.

Interoperability. Applications and computers from different suppliers will have the capability to work together on a network and to connect and share data and processes as appropriate. The model that the standards in this document follow is one that allows end systems to attach to any point on an internetwork. (End systems include clients, servers, and sensors that produce or utilize information.)

Performance. The degree of quality that a particular standard or guidance provides in selecting IM/IT products or services.

Business. Implementation cost and market acceptance of the standard or guidance is also a selection factor. Market acceptance is judged more on market momentum than on current market share. A dominant product may actually be losing market share, while an emerging product or standard may be rapidly increasing its share. By including market acceptance as one of the selection criteria, we obtain a balance in theoretical versus practical value as based on the market conclusions regarding technology, functionality and value.

2.10 Enterprise Standards and Guidance Profiles

The standards profiles specify the standards and implementation approaches to build the systems across the entire IT spectrum, for a DON platform, activity or across the entire enterprise. These profiles include standards and guidance that address critical hardware, software, communications, data management, security, and user interface characteristics. Profiles support interoperability across platforms and applications.

2.10.1 Profiles

A profile is a set of specifications bundled together to describe the technical standard for a function or a service (such as operating systems, network, and data interchange services), and will include minimum criteria for the information and technology that support specific functional requirements. Profiles equate to the lowest level business process, and document agreed-to implementation requirements used in building and operating systems. Systems using the same standards, but different options, will probably not interface correctly. For example, e-mail services would be defined in the DoD Technical Reference Model and would have an associated standards profile that defined required features for e-mail within the agency.

2.10.2 DOD Technical Reference Model

Of particular importance is the DOD Technical Reference Model (TRM) for assembling profiles across the following technology categories:

- Computing Resources

- Information Management
- Applications

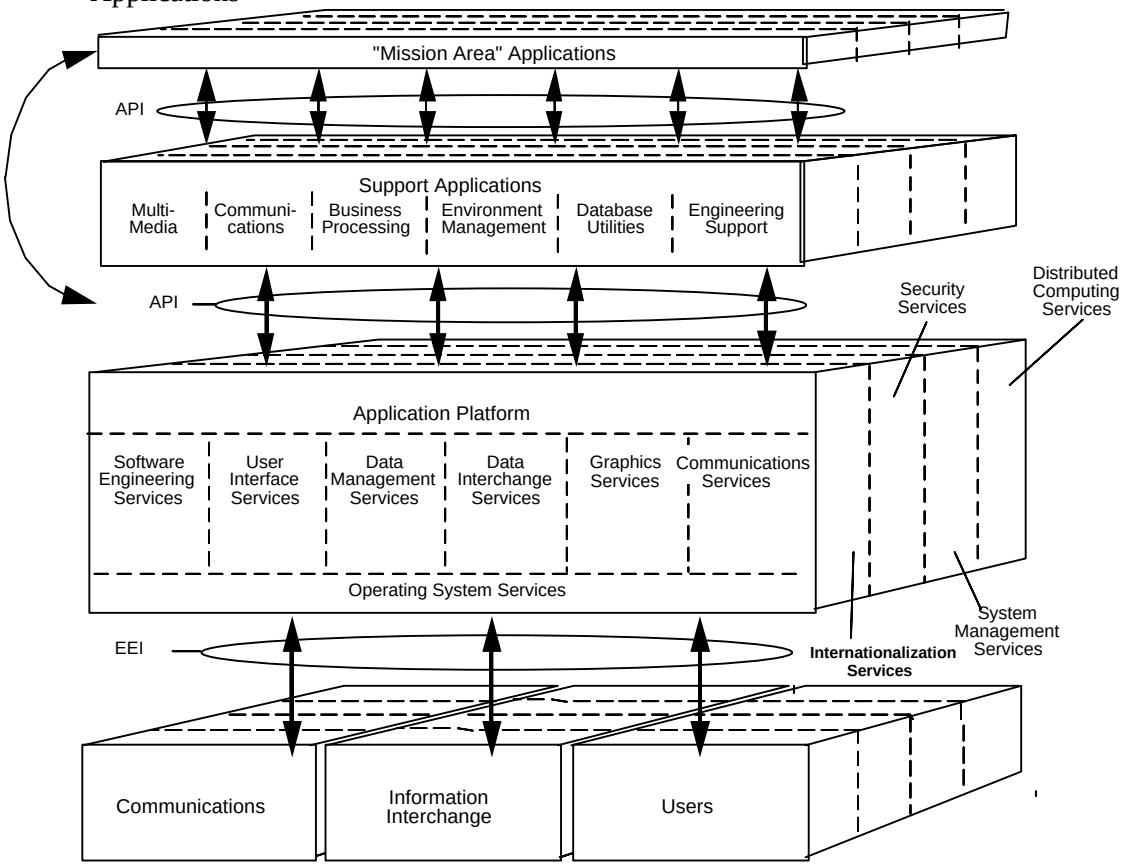


Figure 2-16. DoD Technical Reference Model (Version 3.0)

The DoD TRM shown in Figure 2-16 provides a conceptual framework and common vocabulary of services needed in each of the standards elements. The TRM identifies and specifies the support services (multimedia, communications, etc.) and interfaces that provide a common operating environment and support the flow of information among enterprise and common support applications. This model represents the computer resources, information management and applications categories and interfaces with the communication and networking technology categories that are appropriately represented by the ISO Open System Interconnect model. The DoD TRM addresses standard profiles that provide seamless application support over widely distributed computing resources and attendant interfaces between the computing resources and other technologies. It is important to note that this DoD TRM is platform-centric and cannot be used as the sole framework for a network-centric environment.

2.11 Promulgation of IT Standards and Guidance

Figure 2-17 illustrates how each chapter is organized. As shown, there will be an overview that provides a summary of what is contained in the chapter. Some chapters will also have a background section to provide a foundation to understand the contents. Within the body of the chapter, topics will be introduced and discussed. An associated statement on the implementation of the standard, specification or guidance will be followed by a table showing the recommended implementation over time for different platforms. Each chapter will close with a list of references.

The official references of the standards and guidance will be provided as well as any sources supporting the chapter.

Overview

Background

Topic

Description

Discussion

Best Practices

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Avoid selecting any of these specifications, products, or technologies	Select specifications, products, or technologies based on this time line.				These specifications, products, or technologies are being monitored as potentially significant.
Activities, Platforms, Operational Environments		The specifications, products or technologies above apply to these platforms or operational environments.			

Notes

References

Sources for Standards Guidance

Supporting Resources

Figure 2-17. Generic ITSG Chapter Outline

2.12 References

Joint Staff, J6, “C4I For the Warrior” 12 June 1992

Joint Staff, “Joint Vision 2010, America's Military: Preparing for Tomorrow”; 1996

Chief of Naval Operations (CNO) N6 Copernicus: C4ISR for the 21st Century, September 1997

U.S. Marine Corps “...From the Sea” September 1992

Defense Information Systems Agency (DISA): Joint Defense Information Infrastructure Control Center Concept of Operations (DII CC CONOPS); 22 July 1997

Defense Information Systems Agency (DISA); “Defense Information Infrastructure Common Operating Environment (DII COE);” 1 May 1998; http://spider.osfl.disa.mil/dii/ (24 May 1998)

SPAWAR Systems Center San Diego; “Navy C4ISR Technical Architecture” Version 0.9; 17 September 1997.

3. Information Protection

This chapter includes system and information security standards and guidance. The relationship of this chapter with the ITSG is shown in Figure 3-1.

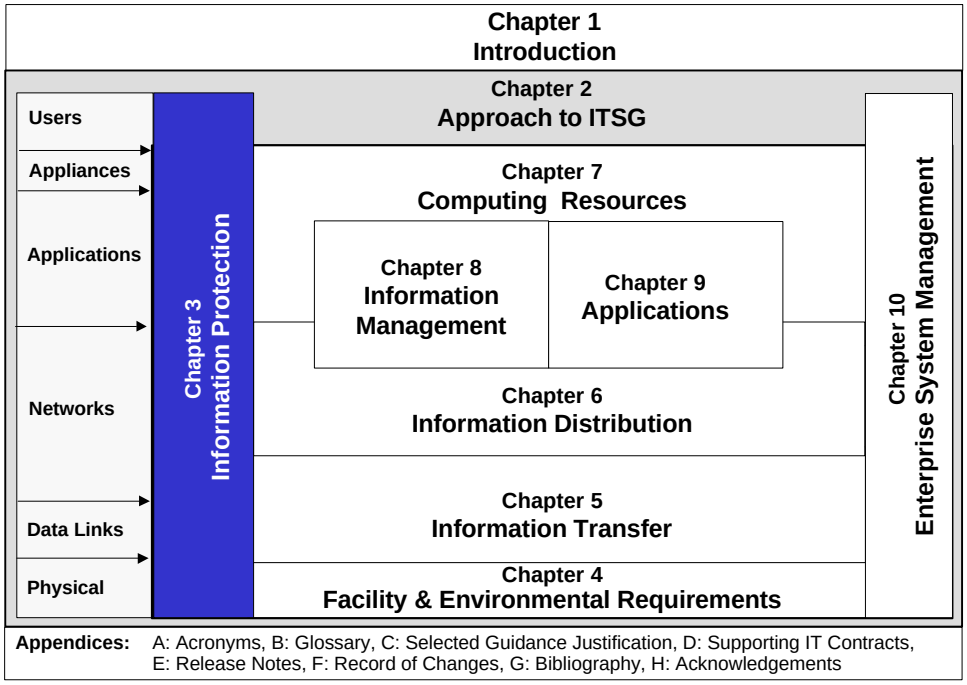


Figure 3-1. ITSG Document Map Highlighting Chapter 3, Information Protection

3.1 Overview

This chapter provides the information protection standards guidance necessary to implement secure information systems while ensuring interoperability. The standards, identified in the “best practices” paragraphs, apply to all DON automated information systems.

3.2 Background

DON information systems must have adequate safeguards, both technical and procedural, to ensure the security of data processed. System safeguards must provide information protections commensurate with the security requirements of the data processed in a particular information system. In general, DON information systems should provide appropriate safeguards to ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of information processed. The actual safeguards used should be commensurate with the operational requirements, information sensitivity level, and consequences of exploitation of the specific DON information system.

Most modern DON information systems are rapidly developed and fielded in an evolutionary manner. The majority of these systems are intended to be connected to LANs and use WANs (e.g. the NIPRNET or SIPRNET) as a primary data transport mechanism. Unfortunately, these LAN/WAN connections can be exploited by an adversary attempting to compromise DON information and information systems. Providing an adequate level of information protection at an

acceptable cost is difficult in this type of environment. Recent experience in the DON, DOD, and private industry has shown that the best solution to this problem is to use a defense in depth approach to information protection.

Defense in depth is provided by employing multiple security mechanisms at various locations (both physical and logical) in an information system. These mechanisms are applied in both a complementary and redundant manner to satisfy the information system's security requirements. No single mechanism is relied upon to provide complete information security. To compromise the security of a DON information system, an adversary must defeat the security mechanisms, "layer-by-layer." Defense in depth is extremely beneficial because most modern DON information systems are composed of COTS operating systems (OS) and applications, and these are regularly discovered to have subtle security flaws. With proper defense in depth, the risk is minimized that a single security flaw in an OS or application will leave an information system vulnerable.

3.3 Information Protection Requirements

Information protection requirements must be defined for each DON information system. The specific requirements are derived from the operational concept of an information system and take into account the system mission, sensitivity of the information processed, and the possible consequences of compromise. The information protection requirements are documented in the information system's security policy. At a minimum, the information system security policy specifies the system-specific information protection requirements in the following areas:

Confidentiality – The protection of classified and sensitive unclassified information from unauthorized disclosure.

Integrity – The protection of information and information system resources from unauthorized, undetected modification.

Availability – The assurance that authorized users will have reliable and timely access to required resources (including information, system services, communication services, etc.).

Authenticity – The ability to determine if information was created or modified by an authorized entity.

Non-repudiation – The ability to provide non-forgeable proof of a data originator's identity and non-forgeable proof of data receipt.

Employing information protection measures satisfies these information protection requirements. There are six broad categories of information protection mechanisms.

Encryption – Converting understandable information into unintelligible data for storage and transport in potentially hostile environments and then restoring this information (decryption) to authorized users.

Access Control – Controlling access to system data and resources based on a user's identity or operational role.

User Identification and Authentication (I&A) – Securely determining a user's identity or operational role.

Malicious Content Detection – Examining incoming data to detect and block malicious content (e.g., viruses).

Audit – Recording security-relevant events in a protected form (for use in non-real-time event reconstruction as well as in real-time intrusion detection).

Physical and Environmental Controls – Policies, procedures, and mechanisms related to physically protecting and providing for continuity of operations for system components. These are addressed in Chapter 4.

To achieve information protection over the DON enterprise, the information architecture can be categorized in dimensions that must be protected. The top level dimensions listed from the more general to the specific are:

Information System – The actual infrastructure itself must be protected against unauthorized intrusion and denial of service.

Information Domain – Communities-of-interest within the infrastructure must be afforded freedom to move and process information within a virtual enclave that provides protection.

Information Content – Information packages themselves have to be protected against unauthorized access by untrusted users both in-transit and at rest (in storage).

Figure 3-2 is a summary of the dimensions and components used to provide information protection. Each dimension is shown as a matrix of information protection requirements (confidentiality, et al) versus information protection measures (encryption, et al). Within each cell of the matrix are components that are used to effect the information protection measures. The concept of these dimensions allows flexible release of some information elements to selected trusted users while protecting the rest of the information from those who do not have a need to know. A defense-in-depth strategy is used to layer security measures at each perimeter of the infrastructure. A collection of security components is used to establish the protection needed at each zone for each information protection dimension.

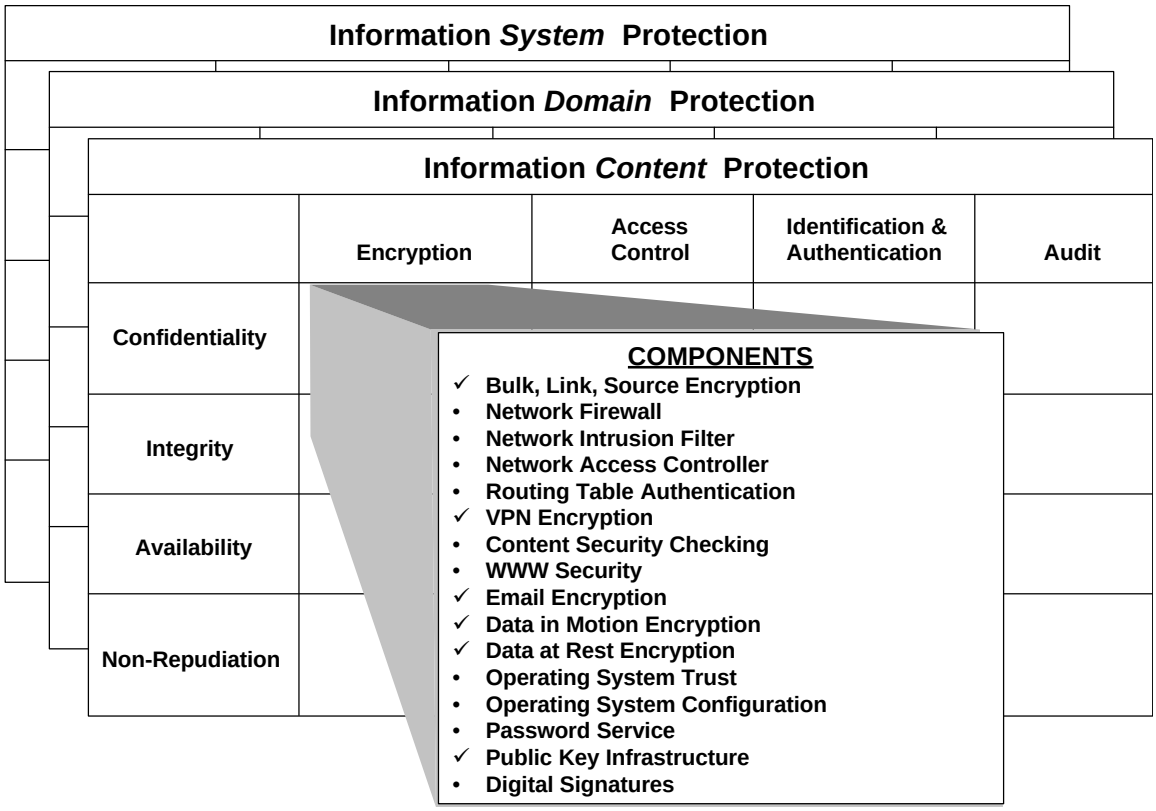


Figure 3-2. Information Protection Summary

3.4 Defense in Depth Approach

In defense in depth, security protection mechanisms are employed in a layered fashion, at multiple locations in a system architecture. This ensures that DON systems maximize resistance to attacks and minimize the probability of a security breach due to a weakness (known or unknown) in any single security mechanism.

The defense in depth information protection concept is directly analogous to sea control concepts. Fleet air defense can serve as a representative example. The outer zone is defended by intercept fighters such as F-14s and controlled by E-2Cs; a second layer of defense is the missile zone defended by Aegis cruisers; they intercept attackers that have not been defeated by the outer layer. Inside the missile zone lie the point defense zones where the defensive weapons include chaff, close in warfare systems and tactical electronic warfare machinery. If the system is working properly, the number of leakers that penetrate to the inner zone is less than the capacity of the point defense weapons.

A generic framework for defense in depth is illustrated in Figure 3-3. Four zones of defense are defined in this framework. It is important to note that the zones of defense may be logical and not necessarily physically separate. It should also be noted that the selection, placement, and configuration of particular security mechanisms are implementation dependent. The type and strength of security mechanisms are driven by the information protection requirements for a particular DON information system.

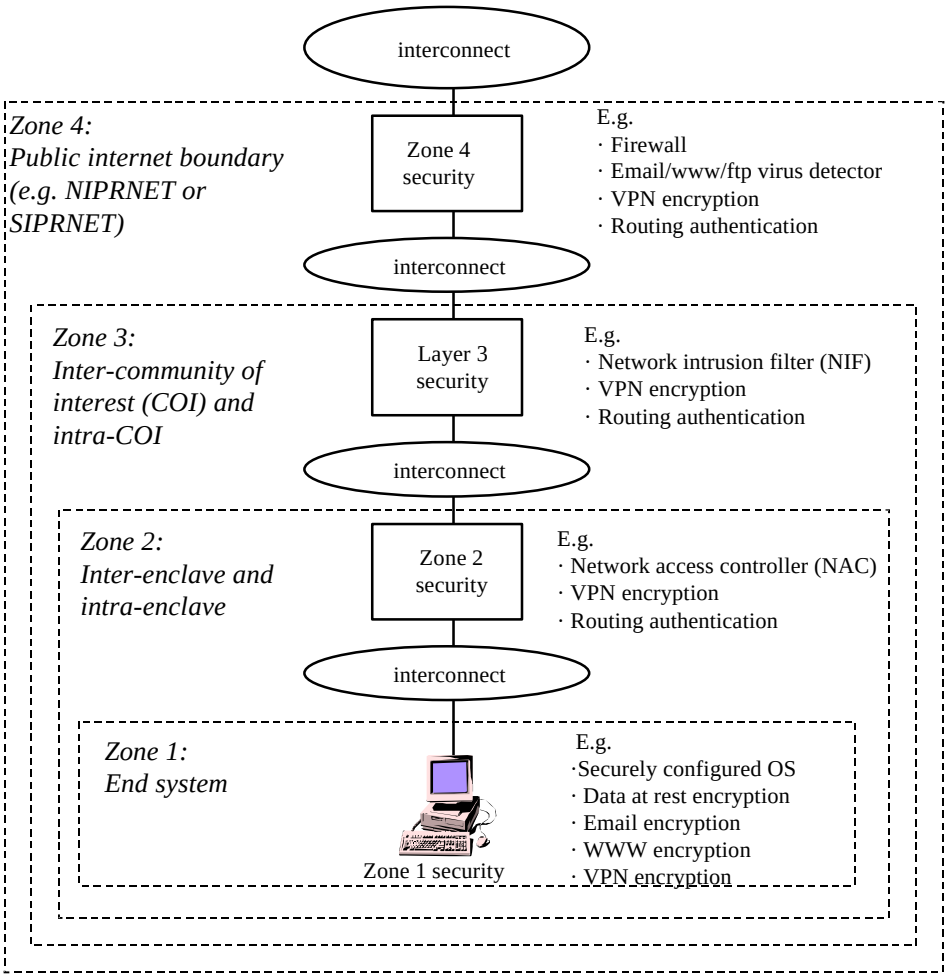


Figure 3-3. Defense in Depth Concept

In addition to the information protection mechanisms, certain infrastructure components are required to build secure DON information systems. The most critical of these components is a public key infrastructure (PKI) that can be applied in the various zones to support identification and authentication mechanisms and encryption mechanisms.

Figure 3-4 summarizes how information protection components are applied to each architecture security zone and information dimension. The role of each in protecting the information and infrastructure is provided below.

	Info System	Info Domain	Info Content	ZONE			
				1	2	3	4
Bulk, Link, Source Encryption	C,I,a	C,I,a	C,I,a				✓
VPN Encryption	C,I,a	C,I,a	C,I,a	✓	✓	✓	✓
Data at Rest Encryption		C,I,a	C,I,a	✓			
WWW Encryption		C,I,a	C,I,a	✓			
Email Encryption			C,I,a,N	✓			
Digital Signatures			C,I,a,N	✓			
Routing Table Authentication	A,a	A,a			✓	✓	✓
Public Key Infrastructure		☑	☑	☑			
Network Firewall	C,I,A,a	C,I,A,a			◯	◯	✓
Network Intrusion Filter	C,I,A,a	C,I,A,a			◯	✓	◯
Network Access Controller	C,I,A,a	C,I,A,a			✓		
Content Security Checking		I,A	I,A	✓	◯	◯	✓
Operating System Security	C,I,A,a	C,I,A,a	C,I,A,a	✓			
Operating System Configuration	C,I,A,a	C,I,A,a	C,I,A,a	✓			
Password Service	a	a	a	✓			✓

C confidentiality **a** authenticity
I integrity **N** non-repudiation
A availability

✓ **applicable** ◯ **optional**
☑ **infrastructure component**

Figure 3-4. Security Components Applied to Architecture Dimensions and Protection Zones

3.4.1 Zone 4 Protection Mechanisms

Zone 4 information protection mechanisms are employed at the boundary between a DON information system (or multiple DON information systems connected by a private intranet) and a public internetwork (e.g. NIPRNET, SIPRNET). Zone 4 information protection mechanisms may include:

- Network firewalls
- Virtual Private Network (VPN) encryption
- Content security checking
- Routing table update authentication

3.4.1.1 Network Firewall

The most effective zone 4 information protection mechanism is the properly configured and managed network firewall. A firewall is a collection of hardware and software components that is used to selectively allow external entities (e.g. users on the Internet) access to information systems located “behind” the firewall. A firewall is installed between an information system (or intranetted systems) and a public internetwork. In addition to providing network access control, a properly configured and managed firewall can provide network intrusion prevention.

There are three primary categories of network firewalls:

- Packet filter

- Stateful packet filter
- Application layer gateway

A packet filter firewall uses a conventional filtering IP router to implement Access Control Lists (ACLs) to restrict incoming and outgoing connections based on the service type and the source/destination of the connections. A packet filter is considered to be the least capable and least secure type of network firewall. A stateful packet filter firewall is similar to a packet filter but it can also use knowledge of higher level protocols to identify and allow legitimate protocols, and to identify and disallow certain network attacks. A stateful packet filter firewall is considered more secure than a packet filter firewall. An application layer gateway firewall, also known as a bastion host firewall, examines incoming and outgoing connections at the application layer using proxies. These proxies can force incoming connections to be authenticated at the firewall as well as blocking most known network attacks. An application layer gateway firewall is considered the most secure network firewall.

Because of the associated expense and management overhead, network firewalls may be installed in central locations (e.g., a regional information technology service center) and shared by DON information systems connected via a private intranet.

Best Practices

All DON information systems should use application layer gateway network firewalls to secure connections to public internetworks. Network firewalls can be centrally located, centrally managed, and shared between multiple sites only if a secure intranet is used to connect the sites. A Memorandum of Agreement (MOA) may be required between the DON activities that share a network firewall. The MOA should state the firewall policies that specify the network services to be allowed (see Figure 3-5 for representative services).

Application layer gateway network firewalls procured for DON information systems should, at a minimum, provide support for the following network applications: SMTP, HTTP, HTTPS, SSL, gopher, NNTP, telnet, FTP, and RealAudio. Network firewalls at a minimum should support secure, non-spoofable, user authentication across a network-MD5 based Skey. Network firewalls should support integration with one of the products on the DoD virus tool site license (see Section 3.4.1.3) using the Open Platform for Secure Enterprise Connectivity (OPSEC) Content Vectoring Protocol (CVP). If a virtual private network (VPN) encryption capability is required, it should conform to policies specified in Section 3.4.1.2 of this document.

Network firewalls should be configured with the most restrictive security policy possible, “that which is not expressly allowed is denied.” Figure 3-5 identifies a baseline of network services that either can, can conditionally (based on system specific requirements), or cannot securely be allowed through a network firewall. It should be noted that although specific protocols may not have a first order negative impact on system security, their use by DON systems may lead to inadvertent denial of service due to resource consumption. As a result, DAAs need to consider if the operational requirement for a particular protocol justifies the potential negative impact on network resources. Detailed guidance documenting the vulnerabilities and risks associated with allowing specific network services to traverse a network firewall can be found in “Firewall Services,” SPAWAR PMW-161 report, December 1996. This report can be accessed at: ftp://infosec.navy.mil/pub/docs/navy/NSS/firewalls/fw_serv.doc.

DON information systems must ensure that any protocols used across public internetworks are compatible with application layer gateway network firewalls. Guidance for determining this compatibility is identified in the “Firewall Services” document.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	Application layer gateway network firewall	Application layer gateway network firewall	Application layer gateway network firewall	Application layer gateway network firewall	
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, Shore Commands connected directly to a WAN			

Table 3-1. Zone 4 Firewall Recommended Implementations

Service	Allow in	Comments	Allow out	Comments
DNS	Yes	Split server	Yes	Split server
SMTP	Yes	Secured mail forwarder	Yes	Secured Mail Forwarder
TELNET	Yes	Proxy with strong authentication	Yes	Proxy
HTTP	Yes	Proxy with strong auth., external server, split server Block ActiveX Conditionally allow Java	Yes	Proxy, IP address filter, Split Server
HTTPS (SSL)	Yes	Proxy, external server, split server Block ActiveX Conditionally allow Java	Yes	Proxy, IP address filter, Split Server
RealAudio™	Yes	Proxy	Yes	Proxy
Lotus Notes	Yes	Generic proxy, IP port filter	Yes	Generic Proxy, IP Port Filter
FTP	Yes	Proxy, strong authentication	Yes	Proxy
WAIS	Cond.	Split server	Yes	Proxy
Anonymous FTP	Cond.	Server external to firewall	Yes	Proxy
SQL*Net	Cond.	Proxy with strong authentication	Yes	Stateful packet filter, proxy
Gopher	Cond	External server, split server	Yes	Proxy, IP address filter, Split Server
NNTP	Cond.	External server, generic proxy	Yes	Generic Proxy
ICMP	Cond.	Block “echo request,” “time to live exceeded,” “redirect.”	Cond.	Block “echo reply,” “time to live exceeded,” “redirect.”
X.400	Cond.	Generic proxy	Cond.	Generic Proxy
X.500	Cond.	Generic proxy, IP port filter	Cond.	Generic Proxy IP Port Filter
DMS	Cond.	Split server	Cond.	Split server
POP3 and IMAP4	Cond.	Proxy with strong authentication	Cond.	Proxy
‘r’ commands	Cond.	Proxy with strong authentication	Cond.	Proxy

Service	Allow in	Comments	Allow out	Comments
IRC	Cond.	Generic Proxy, IP Port Filter	Cond.	Generic Proxy, IP Port Filter
T.120/H.323	Cond.	Generic Proxy, IP Port Filter	Cond.	Generic Proxy, IP Port Filter
Syslog	Cond.	Log at firewall, limit to external router and DON servers inside external router using packet filters	No	
SNMP	No		Cond.	Two mgmt. stations, IP Address Filter, proxy
Finger	No		Cond.	safe_finger
X-Windows	No		Cond.	IP Address Filter
Printing	No		Cond.	Proxy
NTP	No		No	
Microsoft RPC	No		No	
NETBIOS	No		No	
NIS	No		No	
RPC	No		No	
Archie	No		No	
TFTP	No		No	
NFS	No		No	
Talk	No		No	
MBONE	No		No	

Cond. = conditional; service may be acceptable based on system specific requirements

Figure 3-5. Allowable Services for Network Firewalls

3.4.1.2 Virtual Private Network (VPN) Encryption

VPN encryption can be used to provide confidentiality and integrity of data transmitted across a public internetwork. In addition, VPN encryption can provide authentication of the remote system that encrypted the data. When integrated into suitable system architectures, VPN encryption allows secure “tunnels” to be established across insecure internetworks. This allows a private intranet to run (securely) over a public internet.

The National Security Agency (NSA) evaluates the strength of cryptographic devices intended to secure classified data. A VPN encryption device endorsed by NSA for Type 1 applications can be used to encrypt classified networks, providing a resulting data stream that can be treated as unclassified. The NSA endorsed Type 1 devices allow VPN encryption at the IP or ATM layers.

- For IP encryption, there are currently only two NSA endorsed devices – the Network Encryption System (NES) and the Embeddable INFOSEC Product (EIP). NES is a COTS device produced by Motorola. Unfortunately, the NES has performance and key management limitations that have made deployment difficult. EIP is a GOTS device that is centrally procured by OPNAV N6. EIP has not yet been operationally employed and is currently only available in limited quantities.
- For ATM encryption, the only device currently endorsed by NSA, is the Fastlane (KG-75). In FY99, NSA expects to release (and shortly thereafter endorse) a device that will be capable of providing both IP and ATM layer encryption. This device, the Taclane, is expected to overcome the limitations associated with the NES in the IP encryption mode. It will not be interoperable with the NES or EIP in IP layer encryption mode. It will be interoperable with the Fastlane in ATM layer encryption mode, but will operate only at DS-3 rates.

Many commercial vendors produce software and hardware that can provide VPN encryption for unclassified or sensitive but unclassified data. Recently, a number of vendors have developed VPN encryption based on the IP security (IPSEC) standard. IPSEC can provide data confidentiality, integrity, and authentication by encrypting packets at the IP layer.

The IPSEC standard has been designed to allow for “drop-in” employment of encryption algorithms.[1] For data confidentiality, IPSEC currently supports various algorithms including DES, 3DES, RC5, IDEA, CAST128, and Blowfish. For data integrity and authentication, IPSEC currently supports keyed MD5 and SHA-1. The IPSEC standard also allows for employment of various key management and distribution schemes. The simplest is based on manual pre-placement of key material. The Internet Security Association and Key Management Protocol (ISAKMP)/Oakley provides more automated and scalable key management and distribution.

Best Practices

Classified data that is encrypted with VPN techniques must be handled at its original classification level unless an NSA-endorsed Type 1 (designed to secure classified information) cryptographic device is used. If declassification of data is required (e.g. to allow for transmission over non-secure networks), an NSA-endorsed device must be used. Requirements for NSA-endorsed cryptographic devices must be submitted to CNO N643 for validation. Many NSA-endorsed cryptographic devices are centrally procured by SPAWAR PMW-161.

COTS VPN mechanisms may be used for encryption of unclassified data, and of classified data that will be handled at its original level (e.g., for privacy of secret data across the SIPRNET). To provide for interoperability, IPSEC based mechanisms will be used if available. IPSEC mechanisms will utilize DES or 3DES for encryption. FIPS 140-1 certification of DES implementations is recommended. Keyed SHA-1 for data authentication and integrity is preferred, but keyed MD5 is an acceptable substitute if SHA-1 is not available. Additional

[1] An overview of cryptography and DON standards/guidance for cryptography is presented in section 3.6. Standards and guidance provided in section 3.6 apply to all infrastructure components and information protection mechanisms that make use of cryptography.

information on the use of commercial cryptography in DON systems is provided in Section 3.6. An acceptable option for key management and distribution is a preplaced secret key.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary VPN products	IPSEC with • DES or 3DES • SHA-1 or MD5 • Preplaced key or ISAKMP/ Oakley	IPSEC with • DES or 3DES • SHA-1 • Preplaced key or ISAKMP/ Oakley	IPSEC with • DES or 3DES • SHA-1 • Preplaced key or ISAKMP/ Oakley	IPSEC with • DES or 3DES • SHA-1 • Preplaced key or ISAKMP/ Oakley	
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, Shore Commands connected directly to a WAN			

Table 3-2. Zone 4 VPN Implementations

3.4.1.3 Content Security Checking

Many forms of computer information can contain harmful content including viruses, macro viruses, Trojan horse programs, etc. These “malicious programs” can be transmitted across a network in a number of ways including SMTP e-mail attachments, FTP file downloads, and Java applets. Incoming data can be checked for harmful content at the public internetwork boundary.

Numerous COTS products exist that can perform this type of content security checking. These products can be integrated with a zone 4 network firewall system. Two such products, Norton and McAfee, are available on the DoD-wide virus detection tool site license (see http://infosec.navy.mil/)

Best Practices

All DON information systems should employ content security checking mechanisms for e-mail with attachments, FTP data, and http data incoming from a public internetwork. Products from the DoD wide virus detection tool site license should be used. Updated virus detection signatures should be downloaded and installed monthly from the http://infosec.navy.mil or http://infosec.navy.smil.mil web site.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DoD site license virus detection tools	DoD site license virus detection tools	DoD site license virus detection tools	DoD site license virus detection tools	
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, Shore Commands connected directly to a WAN			

Table 3-3. Zone 4 Content Security Checking Implementations

3.4.1.4 Routing Table Update Authentication

IP routers are used to connect LANs and/or MANs to public internetworks. Routers connected to public internetworks must regularly exchange routing table updates across these internetworks. These routing table updates can be spoofed in transmission or forged, thus resulting in denial of service or possibly a network intrusion. Many COTS IP routers feature cryptographic authentication of updates for selected routing protocols. These features can often be used by simply reconfiguring existing routers.

Currently, the BGP and OSPF routing protocols support cryptographic authentication. These routing protocols use a keyed MD5 hash algorithm to provide the cryptographic authentication. Due to weakness in the MD5 algorithm, SHA-1 will likely begin to appear as an option for cryptographic authentication of routing protocols.

Best Practices

All IP routers procured for DON information systems should feature, at a minimum, keyed MD5 authentication for BGP, and OSPF routing protocols. Keyed MD5 authentication should be used between all DON IP routers where possible.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Unauthenticated routing protocols	BGP and OSPF with MD5 authentication	BGP and OSPF with MD5 authentication	BGP and OSPF with MD5 authentication	BGP and OSPF with MD5 authentication	BGP and OSPF with SHA-1 authentication
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, Shore Commands connected directly to a WAN			

Table 3-4. Zone 4 Routing Table Security Implementations

3.4.2 Zone 3 Information Protection Mechanisms

Zone 3 information protection mechanisms are used to provide inter-community of interest (COI) and intra-COI security. In general, zone 3 information protection mechanisms are installed as part of an intranet used to connect end user networks that have similar security requirements and have a common COI. Zone 3 information protection mechanisms may include:

- Network Intrusion Filters (NIF)
- Network firewalls
- VPN encryption
- Content security checking

3.4.2.1 Network Intrusion Filter (NIF)

For high value COIs, a strong layer of defense can be provided by a network intrusion filter. A NIF may be less restrictive than a zone 4 firewall and thereby allow a wider range of network applications to be used, both internal to and across the COI boundary. However, a NIF can detect a wide variety of network attacks and block these attacks. Certain classes of NIFs, known as intrusion detection systems, can provide real time reporting to local security managers and/or to the Fleet Information Warfare Center (FIWC).

Several vendors are currently producing products suitable for NIF applications. These products include stateful filtering routers and active intrusion detection systems.

Stateful filtering routers are similar to normal filtering IP routers. They can be used to allow or disallow incoming packets based on source/destination IP addresses and source/destination TCP ports. In addition, stateful filtering routers use knowledge of higher level protocols to identify and allow legitimate protocols, and to identify and disallow certain network attacks.

Active Intrusion Detection Systems (IDS) also use knowledge of higher level protocols to identify network attacks. When an attack is detected, it can be reported to a central monitoring facility and possibly blocked (e.g., using a TCP connection reset). Depending on its configuration, an active IDS may be able to provide a high level of security in a non-intrusive manner.

Best Practices

Use Network Intrusion Filters to provide information protection mechanisms. No standards currently exist.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	Stateful filtering router Active intrusion detection system	Stateful filtering router Active intrusion detection system	Stateful filtering router Active intrusion detection system	Stateful filtering router Active intrusion detection system	
Activities, Platforms, Operational Environments		ITSCs and Shore Information Producer Commands, COIs with strong security requirements			

Table 3-5. Zone 3 Network Intrusion Detector Implementations

3.4.2.2 Network Firewall

COIs with extremely high security requirements may employ network firewalls at zone 3. This will provide increased security but may limit the range of network applications that can be used intra-COI and (more likely) inter-COI. See Section 3.4.1.1 for guidance on network firewalls.

3.4.2.3 VPN Encryption

VPN encryption may be employed at zone 3 to provide COI security across a DON intranet shared with other COIs and/or across a public internetwork. See Section 3.4.1.2 for guidance on VPN encryption.

3.4.2.4 Content Security Checking

Content security checking may be employed at zone 3 to protect entire COIs. See Section 3.4.1.3 for guidance on content security checking.

3.4.3 Zone 2 Information Protection Mechanisms

Zone 2 information protection mechanisms are used to provide security at the boundary to a single site or enclave and on the LAN for the site or enclave. Zone 2 mechanisms are generally integrated as part of the site/enclave LAN. Zone 2 information protection mechanisms may include:

- Network Access Controllers (NAC)
- NIFs
- Network firewalls
- VPN encryption
- Content security checking

3.4.3.1 Network Access Controller (NAC)

A network access controller provides a basic level of access control over network connections based on a site/enclave's local security policy. These controls could include restrictions on incoming connections as well as on connections between LAN segments internal to the site/enclave. These restrictions could be based on the source and destination addresses of the IP packet as well as the service type (e.g., SMTP e-mail, telnet, HTTP). A NAC could be implemented using the organic filtering IP routers used to connect the site/enclave to the external world. For ATM systems featuring "cut through" routing, filtering ATM switches (being developed by at least one vendor) could be used to implement a NAC.

Best Practices

IP routers procured for DON information systems should have the capability to perform IP packet filtering. At a minimum, routers should be able to accept/reject packets based on protocol type, source IP address, destination IP address, source TCP/UDP port, destination TCP/UDP port, and TCP established bit. Routers should be able to audit IP packets rejected by packet filters.

Currently, few options exist for filtering ATM switches. However, as products become available, selection criteria should be similar to that for filtering IP routers (see previous paragraph).

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	Filtering IP router	Filtering IP router	Filtering IP router	Filtering IP router	Filtering ATM switch
Activities, Platforms, Operational Environments		All			

Table 3-6. Zone 2 Network Access Controller Implementations

3.4.3.2 Network Firewall and NIF

Sites/enclaves with extremely high security requirements may employ NIFs or network firewalls at zone 2. This will provide increased security but will increase cost and management overhead. In addition, a network firewall may limit the range of network applications that can be used across the site/enclave boundary. See Section 3.4.1.1 for guidance on network firewalls and Section 3.4.2.1 for guidance on NIFs.

3.4.3.3 VPN Encryption

VPN encryption may be employed at zone 2 to provide COI security across a DON intranet shared with other COIs and/or across a public internetwork. See Section 3.4.1.2 for guidance on VPN encryption.

3.4.3.4 Content Security Checking

Content security checking may be employed at zone 3 to protect entire sites/enclaves. See Section 3.4.1.3 for guidance on content security checking.

3.4.4 Zone 1 Information Protection Mechanisms

Zone 1 information protection mechanisms provide the inner-most layer of defense for DON information systems. The protections are implemented on the actual end systems including NT workstations, NT servers, UNIX servers, and mainframes. Zone 1 information protection mechanisms may include:

- Secure operating systems with secure configurations
- Data at rest encryption
- E-mail encryption
- World Wide Web (WWW) encryption
- VPN encryption
- Content security checking

3.4.4.1 Operating System Security Features and Configuration

Computer operating systems used in DON information systems should include features that allow the operating systems to provide access control for all information stored or processed. The National Security Agency (NSA) provides specification for security features and criteria for their

evaluation in DoD 5200.28-STD, commonly known as the Orange Book. The Orange Book C2 level specifies the minimum features required to provide access control in a multi-user environment: user identification and authentication, discretionary access control (DAC) with object reuse, and audit. An interpretation of the Orange Book C2 level requirements for DON information systems is provided in DON NAVSO P-5239-15 “Controlled Access Protection (CAP) Guidebook.”

Many COTS operating systems have been designed to meet C2 level requirements and some have been formally evaluated by NSA. Microsoft Windows NT 3.5 has been formally evaluated to meet C2 level requirements by NSA. Microsoft is currently seeking a formal NSA evaluation of NT 4.0 and has indicated formal evaluation will be sought for NT 5.0. Netware 4.11 has been formally evaluated to meet C2 level requirements by NSA and it is anticipated that Netware 5.0 will be entered into formal evaluation as well. Older versions of UNIX operating systems from various vendors have been formally evaluated to the C2 level by NSA. The current versions of most vendors’ UNIX operating systems have not been formally evaluated by NSA. However, these versions of UNIX generally contain C2 level features.

Security features of operating systems should be configured in a standardized manner to provide the highest level of security possible. These configurations should be periodically checked via an automated mechanism and reapplied as required.

Operating systems that do not contain C2 level security features (including Windows 3.1, DOS, Windows 95, Windows 98, Macintosh OS) should be avoided if possible. However, in situations where a PC will be normally used by a single person with no or limited network connections (e.g. a laptop), these operating systems may be acceptable if operating systems with C2 level features cannot meet the system functional requirements. Consult DON NAVSO P-5239-15 for detailed information that can be used in making such a determination.

DON information systems using Windows NT 4.0 (workstation and server) should be configured according to Naval standard configuration guidance. This guidance is documented in “Secure Windows NT Installation and Configuration Guide,” SPAWAR PMW-161 report, November 1997 (or the latest version). This report can be accessed at ftp://infosec.navy.mil/pub/docs/navy/NT-SECURITY/navynt.zip

DON information systems using UNIX should follow best commercial practices for security configuration. Information on this topic can be accessed at: ftp://infosec.navy.mil/pub/docs/unix/.

Best Practices

Computer operating systems used in DON information systems should include C2 level security features. Formal NSA C2 evaluation is not required but is desirable. DON NAVSO P-5239-15 should be used in determining the suitability of a particular operating system.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Operating Systems without C2 features	Windows NT 3.5/4.0 Netware 4.11 UNIX	Windows NT 4.0 Netware 4.11/5.0 UNIX	Windows NT 4.0/5.0 Netware 4.11/5.0 UNIX	Windows NT 4.0/5.0 Netware 4.11/5.0 UNIX	
Activities, Platforms, Operational Environments		All			

Table 3-7. Operating System Security Implementations

3.4.4.2 Application Layer Data at Rest Encryption

Encryption of data files stored on a workstation or server can provide defense against unauthorized access attempts originating both locally (e.g. browsing) and remotely (e.g. hacking across the Internet). Numerous COTS software and software/hardware-based encryption products are available. Most products can be configured to encrypt either on command or automatically (on file open and close).

Although many COTS data at rest encryption products utilize standard algorithms for encryption (e.g. DES), no standards exist for encrypted file formats. This makes interoperability between products impossible.

Best Practices

DON information systems that make use of data at rest encryption products should only employ products that use the following symmetric data encryption algorithms: DES, Triple DES (3DES), or Skipjack. See Section 3.6.2 for more information on acceptable encryption algorithms.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Products with proprietary encryption algorithms	DES, 3DES, or Skipjack based products	DES, 3DES, or Skipjack based products	DES, 3DES, or Skipjack based products	DES, 3DES, or Skipjack based products	
Activities, Platforms, Operational Environments		All			

Table 3-8. Data at Rest Encryption Implementations

3.4.4.3 E-mail Encryption

Encryption can be employed by various applications to provide confidentiality, integrity, authentication, and non-repudiation for information transmitted across a network. One of the best

examples of this is application layer encryption of internet e-mail with attachments. Numerous COTS products exist that provide e-mail encryption. Some are based on proprietary schemes for encryption and limit interoperability. However, standards for e-mail encryption are now appearing along with interoperable products based on these standards.

Secure MIME (S/MIME) provides a developing set of standards for security of internet e-mail with attachments. S/MIME provides for the authentication of the mail sender and the protection of the integrity of the message content (both provided via a digital signature). It also provides for the confidentiality of the message body (provided by encrypting the message). The digital signature and the key are both based on public key cryptography. The encryption of the message body is based on symmetric cryptography.

S/MIME Version 2 is widely implemented and a number of vendors have passed interoperability tests. S/MIME v2 has not been approved by any recognized standards body; the standard is published as two documents called Internet-drafts by a group of e-mail and security software vendors. For a variety of reasons, S/MIME v2 will not become an Internet (IETF) standard, but as a de facto standard is supported by many popular e-mail products.

The next version of S/MIME (version 3) is being developed by the IETF S/MIME working group and is expected to become an IETF standard. This version of S/MIME may be used in web browsers and other Internet applications (for instance to allow the signing of documents) as well as in electronic mail. S/MIME version 3 is not yet available in commercial products. However, the standardization process is proceeding rapidly and may be in products in 1999. This ITSG classifies S/MIME v3 as an emerging standard.

Best Practices

E-mail encryption deployed in DON information systems should avoid proprietary solutions that preclude interoperability. Deploy only S/MIME-based solutions (currently S/MIME v2, possibly S/MIME v3 in the future).

In order to ensure that Naval organizations can trust the digital signatures in S/MIME messages, the digital certificates used must come from a Certificate Authority (CA) recognized by the Navy and Marine Corps as conforming to acceptable certificate issuance practices. Navy and Marine Corps organizations interested in CA pilot projects should contact the Navy INFOSEC Program Office, SPAWAR PMW-161. The S/MIME clients should be configured to recognize only the conforming certificate authorities. Many S/MIME clients come configured to recognize many of the current commercial certificate authorities; these may or may not conform to DoD or Naval CA standards.

Users of S/MIME v2 should be trained to check the identity of the signer (usually by examining the certificate that arrived with the e-mail), and to check the proper Certificate Revocation List (CRL) on the proper directory to ensure that the certificate used has not been revoked.

The cryptographic options selected should be from the following list since not all of the cryptography available in S/MIME v2 products is sufficiently strong to be used for DON applications. The following options are acceptable:

- DES EDE3 encryption in Cipher Block Chaining (CBC) mode with a 168-bit key (Triple DES or 3DES)
- DES encryption in CBC mode with a 56-bit key

The following S/MIME v2 encryption options should be considered UNACCEPTABLE for DON use:

- RC2 encryption in CBC mode with a 128-bit key
- RC2 encryption in CBC mode with a 64-bit key
- RC2 encryption in CBC mode with a 40-bit key

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary e-mail encryption products SMIME with RC2 encryption	SMIME with DES or 3DES encryption	SMIME with DES or 3DES encryption	SMIME with DES or 3DES encryption	SMIME with DES or 3DES encryption	SMIME v3
Activities, Platforms, Operational Environments		All			

Table 3-9. E-mail Encryption Implementations

3.4.4.4 World Wide Web (WWW) Encryption

Another application that can significantly benefit from application layer encryption is WWW. Extensive deployment of WWW servers for both tactical and non-tactical applications is ongoing. The *Secure Sockets Layer (SSL)* protocol provides for both parties in a web-based transaction to authenticate each other and to hide communication via encryption of the information flowing between server and client. SSL can provide for fine-grained access control to web sites (by requiring a user to provide a valid certificate) and signatures, authenticity and privacy for transactions involving web browsers and servers. An interesting feature of SSL is that for the transaction in which the browser user's identity is not important, but encryption of the transaction and the authenticity of the web server are, only the server needs a valid certificate.

SSL v2 was the first widely deployed version of SSL. Most web servers and web browsers support SSL v2. It has been replaced by SSL v3, but not all servers and/or browsers support v3, although all current version browsers and servers support v3. It is a de facto standard, rather than one issued by a recognized standards body, but it is widely deployed.

Best Practices

Navy and Marine Corps web browsers and servers that use SSL should be configured to enable SSL v3 only. However, in those limited situations in which SSL v2 must be used, only the modes that employ stronger encryption should be used. Commands should move as rapidly as possible to products that use SSL v3; SSL v2 will only be acceptable for use for a limited time. Considerations for certificate issuance are similar to those for S/MIME systems (see Section 3.4.4.3).

Versions of web browsers or servers sold for export are not acceptable for use in the Navy and Marine Corps because of their lack of strong encryption. Web browsers or servers that

incorporate stronger encryption generally also include weak encryption. The browser should be configured so that weak encryption is not allowed.

In the web browser or web server, the following options for SSL v2 are acceptable:

- Triple DES (3DES) encryption with a 168-bit key
- DES encryption with a 56-bit key

The following options should be considered UNACCEPTABLE for DON use of SSL v2:

- RC4 encryption with a 128-bit key
- RC2 encryption with a 128-bit key
- RC4 encryption with a 40-bit key
- RC2 encryption with a 40-bit key

In the web browser or server, the following options for SSL v3 are acceptable:

- Triple DES (3DES) encryption with a 168-bit key and a SHA-1 MAC
- DES encryption with a 56-bit key and a SHA-1 MAC

The following options should be considered UNACCEPTABLE for DON use of SSL v3:

- RC4 encryption with a 128-bit key and an MD5 MAC
- RC4 encryption with a 40-bit key and an MD5 MAC
- RC2 encryption with a 40-bit key and an MD5 MAC
- No encryption with an MD5 MAC

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
SSLv2 and SSLv3 with RC2 or RC4 encryption	SSLv2 with DES or 3DES SSLv3 with DES or 3DES	SSLv3 with DES or 3DES	SSLv3 with DES or 3DES	SSLv3 with DES or 3DES	
Activities, Platforms, Operational Environments		All			

Table 3-10. WWW Encryption Implementations

3.4.4.5 VPN Encryption

VPN encryption can be provided at zone 1 as well as zones 2, 3, and 4. By placing VPN encryption in zone 1, data can be secured end-to-end. This can provide an extremely high level of security, especially in situations where LAN cables are not fully secured. See Section 3.4.1.2 for guidance on VPN encryption.

3.4.4.6 Content Security Checking

Content security checking can also be provided at zone 1. In many situations, full content checking in zones 2, 3, and 4 may not be possible due to VPN or application layer encryption. In addition, only zone 1 based content security checking can be used to protect workstations from malicious programs that are imported on floppy disks, CDROM, ZIP drives, tapes, or other removable media. The DoD-wide virus detection tool license allows installation of the DoD licensed tools on home computers as well. Checking content on these computers (which may not be behind appropriate zone 2, 3, and 4 protections) before moving the content to official Navy and Marine Corps computers can help protect Navy and Marine Corps workstations.

Best Practices

All DON PC based workstations and servers (including those using the Windows NT, Windows 95, Windows 98, and Macintosh operating systems) should employ content security checking mechanisms from the DoD-wide virus detection tool site license. Content security checking mechanisms should be configured to run in a background mode and scan files upon access. Updated virus detection signatures should be downloaded and installed monthly from the http://infosec.navy.mil or http://infosec.navy.smil.mil web site.

DON organizations should strongly encourage DON employees to install the DoD-licensed antiviral software on the employees' home computers. Organizations should publicize that this software is available free for home use of DON employees.

DON organizations should consider implementing procedures requiring files to be virus scanned before they are attached to outgoing e-mail. A record of the time and date of the scan as well as the tool used should be included in the body of the e-mail.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DoD site license virus detection tools	DoD site license virus detection tools	DoD site license virus detection tools	DoD site license virus detection tools	
Activities, Platforms, Operational Environments		All			

Table 3-11. Content Security Checking Implementations

3.5 Public Key Infrastructure

The defense in depth approach to information protection for DON information systems is based on the application of numerous complementary and redundant security mechanisms. In addition, infrastructure components are required to support and manage these security mechanisms. The most critical of these components is a Public Key Infrastructure (PKI) required to support the multiple encryption mechanisms that can be applied in the various zones (e.g. VPN encryption, SMIME, SSL).

A public key infrastructure is a collection of components that support the generation and distribution of digital certificates, issuance of Certificate Revocation Lists (CRLs), and the building and running of directories to serve these certificates and CRLs. In order to understand the operational issues and to develop the proper policies associated with operating a PKI, a number of Naval, DoD, and other government entities are operating PKI pilot projects based on commercial standards. These pilots are called “medium assurance” PKI pilots based upon the level of assurance postulated in the digital signatures associated with the certificates. The Defense Message System (DMS) project is fielding a separate PKI based partially on commercial standards and partially on DMS unique standards (this pilot project is sometimes called a “high assurance” PKI).

A digital certificate is an electronic proof of identity that can be used to sign electronic documents, to authenticate the holder of the certificate, and to allow decryption of information intended to be read by the holder of the certificate. Digital certificates are used in many commercial products (e.g., SSL for WWW security, S/MIME for e-mail security) and are based on the use of public key cryptography. In a public key cryptographic system, a person (e.g., using a web browser) generates a public key/private key pair. The private key is never revealed to anyone and is protected by the application that generated it (in our example, the browser). The public key can then be published (e.g., in an X.500 database).

In order to avoid the problem of hostile impersonators publishing public keys under false names, a person’s name and public key are placed in an electronic document and the document is digitally signed by a widely recognized trusted agent. The agent’s signature binds the person’s name to the person’s public key by virtue of the integrity protection provided by the digital signature. This document is called a *digital certificate* and serves as an electronic credential. Anyone accessing the certificate can (1) verify the signature of the trusted agent and, thereby, verify that the public key and the associated identity have not been modified, (2) know that information encrypted with the public key can only be decrypted by the person (or organization) named in the certificate, and (3) check documents signed by the person to verify the person’s signature. The trusted agent that signs the digital certificate is called a *certificate authority (CA)*. In generating a digital certificate, the CA should carefully verify the associated person’s identity in order to provide the required validity of the certificate. This verification is often performed by another entity called a registration authority (RA). The RA communicates the results of the identity verification to the CA before a certificate is issued.

The certification authority sets necessary restrictions on a digital certificate (e.g., the time interval over which the certificate is valid, typically a year for commercial CAs) and revokes the certificate when appropriate (e.g., when an employee leaves an organization or is no longer authorized to sign documents). The CA publishes a certificate revocation list that can be checked by applications (and persons) when validating a certificate from another entity (i.e., before making purchases from an on-line catalogue company). Persons who rely on digital certificates as proof of identity (signature) and integrity should also check to determine the certificate’s period of validity. And finally, persons who rely on digital certificates must trust that the issuer of the certificate (the CA and possibly the RA) has followed acceptable procedures verifying the identity of the certificate holder. Since a digital signature may be used to sign a legally binding document, strict standards for the certificate issuing process are required.

Certificates and certificate revocation lists are generally stored in a publicly accessible directory that is often based on the X.500 and/or the Lightweight Directory Access Protocol (LDAP).

The X.509 standard specifies the structure and contents of a digital certificate. It includes a number of required fields (including name and public key) and optional fields. Most commercial products that use certificates, require certificates to conform to this standard. However, owing to differences in how certificates are used (differences between SSL and S/MIME for example), the content of the optional fields and their uses may vary. The DMS certificate format is based on a variation of the X.509 standard.

Standards for a CA include definitions of the various identity verifications, certificate issuing, certificate management (including revocation), and due diligence procedures for a CA and any associated registration authorities. These procedures and processes are defined in a standards document called a Certification Practices Statement (CPS).

In order to provide a uniform level of confidence in the signatures for the certificates issued by the various government PKI's, procedures must be standardized. The government PKI pilots are expected to develop a standard CPS for government PKI. Examples of possible certificate issuance and certificate revocation processes are illustrated in Figure 3-6 and Figure 3-7. These may not be representative of the certificate issuance and certificate revocation processes that evolve from the government PKI pilots.

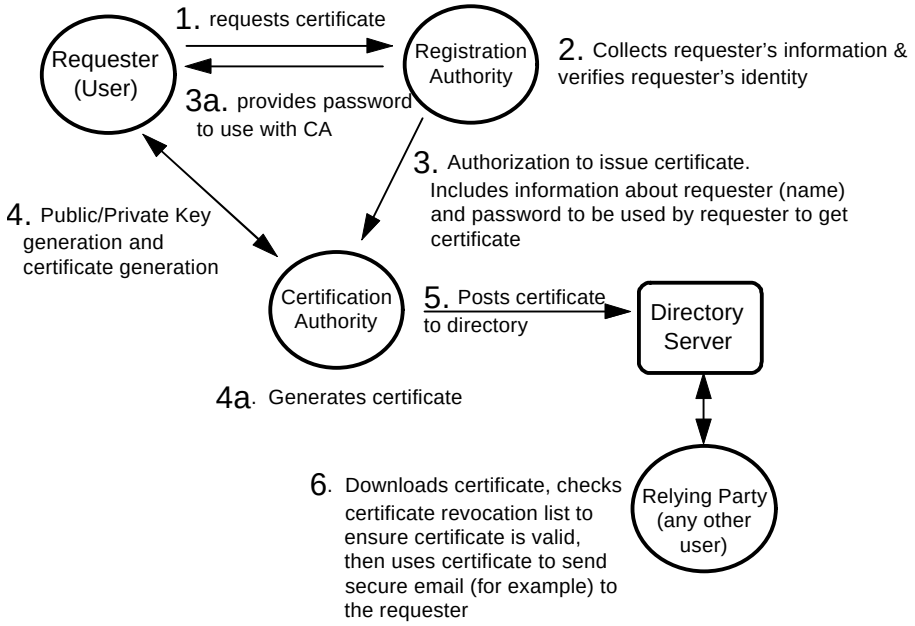


Figure 3-6. Example Certificate Issuance Process

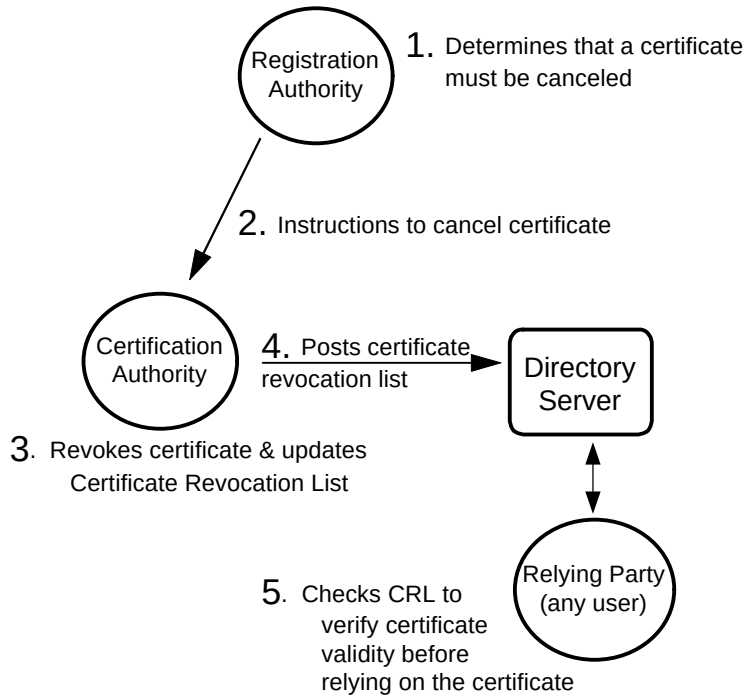


Figure 3-7. Example Certificate Revocation Process

The standards for a PKI also include the standards for the protocols and algorithms used in the communication between and among the CA, RA, and end users' applications. Commercial standards bodies are still developing many of these protocol standards.

Products based on public key cryptography store the private key of the end-user in the product (e.g., a web browser stores the user's private key). An industry standard for securely moving private keys between applications (e.g., between a web browser and a secure e-mail package) is emerging. The use of this standard allows a person to own a single personal digital certificate rather than requiring a different certificate for each application program. The standard is published as part of the Public Key Cryptography Standards (PKCS) of RSA Data Security, Inc. It has been designated PKCS 12.

Best Practices

Owing to the lack of PKI standards, Navy and Marine Corps organizations desiring to use certificate-based public key technologies (e.g. S/MIME, SSL) should coordinate with SPAWAR PMW-161 to either join an ongoing Naval or DoD pilot project or to start a new pilot project.

Navy and Marine Corps organizations using digital certificates should use X.509v3 certificates whenever possible. If possible, the CA's signature should be based on the Digital Signature Standard (DSS). However, until more DSS-based products are available, a signature based on the RSA algorithm is also acceptable.

Naval organizations should use PKCS 12 when private keys are shared between applications.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	X.509v3 certs RSA or DSS for CA signature PKCS12 for key sharing	X.509v3 certs RSA or DSS for CA signature PKCS12 for key sharing	X.509v3 certs RSA or DSS for CA signature PKCS12 for key sharing	X.509v3 certs RSA or DSS for CA signature PKCS12 for key sharing	
Activities, Platforms, Operational Environments		All			

Table 3-12. Public Key Infrastructure Implementations

3.6 Use of Commercially Available Cryptography

Encryption is utilized in numerous information protection mechanisms in all zones and in infrastructure components required to support these mechanisms. This section provides an overview of the best commercial practices in cryptography to protect information (both unclassified information and classified information that will be handled at its original classification level[2]), to make and verify digital signatures, to verify the integrity of information, and to provide other business oriented cryptographic functions. The standards and guidance specified in this section apply to all infrastructure components and information protection mechanisms that make use of cryptography.

The use of cryptography is just one piece of an overall protection strategy. Each piece of the strategy must be considered when determining the level of risk associated with the use of the strategy. Whether or not a particular type of cryptography meets the risk management needs of a particular application depends on many factors, including the strength of the cryptographic algorithm, correctness of the algorithm and associated key management implementation, and the security of the associated *cryptographic protocol*.

The availability and usability of commercial cryptography and security products is increasing. Available products and cryptographic algorithms vary widely in strength and in the quality of implementation. Many commercial cryptographic products are insufficiently strong to provide even weak protections (or signatures, or integrity, etc.). Even many of the products that incorporate strong cryptography allow the cryptography to be used in weak ways. Careful selections of algorithms, of protocol standards, and of product configuration options are all necessary for acceptable security protections.

The following sections provide an overview of cryptography, discuss the acceptable encryption algorithms, and discuss the options required for the secure use of these algorithms. Navy and Marine Corps commands contemplating the use of cryptography for unclassified applications should use the options specified here.

[2] Cryptography used to declassify DoD classified information must be approved by NSA. Contact the Navy INFOSEC Program Office, SPAWAR PMW-161 for further information.

3.6.1 Overview of Cryptography

Cryptographic systems can be divided into two primary types. *Symmetric cryptographic systems* (or secret or private key systems) require the sender and any receivers of a document to have the same key. Securely distributing the secret key to everyone who needs it has historically been a major difficulty with symmetric cryptographic systems. In contrast, *public key cryptographic systems* (also called asymmetric systems) use different keys for the encryption and decryption functions. The encryption key can be made public, allowing anyone with access to the public key to encrypt information intended to be read only by the holder of the private decryption key. If a public key system is used in reverse, it can be used to verify the identity of an information source. The holder of the private key uses it to encrypt information; anyone with access to the public key can decrypt, but since only one person holds the private key, the encrypted document can be tied to the holder of the private key.

In practice, public and private key technologies are often used together. The public key system is used to transmit keys that are then used in a symmetric cryptographic scheme. Public key systems are also used to sign documents. In a typical application, the information to be signed is compressed using a *message digest algorithm* (also called a *secure hash algorithm*). The compressed message (the *message digest*) is signed by being encrypted with the private key piece of a public key scheme. Anyone receiving the document can recompute the message digest, then check the signature using the sender's public key. If the locally computed digest matches the one that arrived with the message, a receiver can determine the identity of the sender (i.e., the document's authenticity) and that the message was not modified en route (i.e., the document's integrity).

A digital signature is a cryptographically produced sequence that a recipient can use in good faith (and hopefully with as low risk as a paper signature) as evidence that a particular person signed an electronic document. Digital signatures are made by using both public key cryptography and message digest algorithms. The document to be signed is put through a message digest function, then the message digest is encrypted with the signer's private key, and the encrypted digest is appended to the document. A recipient uses the signer's public key to decrypt the message digest, puts the document through the same message digest algorithm used by the sender, and if the decrypted digest matches the newly computed digest, concludes that the document arrived unmodified, and that the sender had signed the document.

3.6.2 Standards for Symmetric Encryption Algorithms

The official U.S. government standard for the protection of unclassified information by cryptography is the Data Encryption Standard (DES). DES is the most widely used cryptographic algorithm in the world. Many other symmetric algorithms have been developed commercially, often to meet a perceived need for algorithms that are stronger than DES. However, only a very few of these algorithms have been intensively cryptanalyzed and few have existed long enough to have confidence in their security.

Data Encryption Standard (DES)

As the official U.S. Government standard algorithm for the protection of unclassified information, DES is widely available in commercial products.

Best Practices

DES is currently the preferred symmetric encryption algorithm for the protection of Naval unclassified information. Navy and Marine Corps users should select DES-based products that have been evaluated for proper implementation and operation in accordance with NIST FIPS PUB 140-1, *Security Requirements For Cryptographic Modules*.

DES can be used in a variety of modes. Generally, if a product includes an option for the DES mode, Navy and Marine Corps users should not use DES in the Code Book mode. Other modes have superior security properties.

If a product includes DES and other symmetric algorithms, DES should be used in lieu of the other algorithms unless a careful, risk management analysis is made that determines one of the other algorithms provides lower risk. If an algorithm other than DES is contemplated, it should be selected from the other symmetric algorithms defined in the ITSG and the algorithm should be configured according to the guidance given herein (e.g., key length, number of rounds).

Triple DES

A non-government-standardized variant on the DES algorithm is triple-DES (or 3DES). This scheme encrypts by applying the DES algorithm three times, with three different keys in an attempt to make the key size larger (DES key size is 56 bits, triple-DES is 168 bits) and the cryptography harder to break. The security of the scheme may be better than normal 56 bit DES and is almost certainly no worse. No NIST FIPS for the use of triple-DES exists.

Best Practices

Navy and Marine Corps users may select triple-DES in lieu of DES in applications.

Skipjack (Fortezza)

The Skipjack algorithm is an algorithm developed by NSA and built into Fortezza cards. A number of commercial products can use Skipjack (via the Fortezza card) for symmetric encryption. Many of these products are associated with the Defense Message System program. The Skipjack algorithm is currently classified and so is only available in hardware form. However, the NSA has recently signaled its intent to provide software versions of Skipjack to builders of commercial information processing products. It is unknown at this time whether the FIPS 140-1 quality standard would be applied to these software implementations, or whether NSA and/or NIST will develop a new evaluation standard.

Best Practices

Navy and Marine Corps users may use Skipjack/Fortezza in lieu of DES. However, when commercial products appear that incorporate software versions of Skipjack, the potential user of the product should ensure the product meets whatever quality standard that NIST or NSA has defined (in order to ensure the implementation is correct).

Other symmetric algorithms

Many other symmetric algorithms may be found in commercial products. The security of some of these algorithms is poor and the security of other algorithms may be unknown (not sufficiently cryptanalyzed).

Best Practices

No other symmetric encryption algorithms are approved for Naval use.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary or other unlisted algorithms	DES 3DES Skipjack	DES 3DES Skipjack	DES 3DES Skipjack	DES 3DES Skipjack	
Activities, Platforms, Operational Environments		All			

Table 3-13. Symmetric Encryption Algorithm Implementations

3.6.3 Standards for Public Key Cryptography

The current standards for public key cryptography are not issued by a recognized standards body, but are issued by RSA, Incorporated. The IEEE is developing an IEEE standard for public key cryptography (IEEE P1363: Standard for Public-Key Cryptography) that was issued as a first draft on December 19, 1997 and is expected to be finalized soon. Until the IEEE standard is issued, the RSA standards will be used.

RSA Public Key Cryptographic Algorithm

Many commercial products use RSA cryptography as part of a digital signature scheme and as a way of encrypting and distributing keys that are used in symmetric algorithms (e.g. DES). In the cryptographic literature, the RSA algorithm is considered quite strong as long as appropriate key lengths are selected. No federal government standard exists for the use of RSA. The digital signature standard, FIPS pub 186, defines a digital signature scheme that is NOT based on RSA.

Best Practices

Since the DSS is not yet incorporated into many commercial products, the RSA digital signature is acceptable for use when DSS is not available, but only for a limited time (see Section 3.6.5 on digital signatures).

The use of RSA is acceptable for key exchange and key protection applications.

The minimum key length for Naval applications using RSA is 1024 bits. Longer key lengths provide more protection so longer key lengths should be considered when making risk management decisions about an overall system design.

The use of RSA to protect key material should be done in accordance with both the RSA, Inc. specification for the RSA algorithm and the RSA, Inc. specification for cryptographic message syntax (PKCS #1 and PKCS #7).

Diffie Hellman (DH) key agreement standard

The Diffie Hellman key agreement algorithm is another way of securely exchanging a key that then is used in a symmetric algorithm. It is not widely fielded in commercial products (although the Digital Signature Standard (DSS) is based on a variation of DH).

Best Practices

Navy and Marine Corps users may use the Diffie Hellman key agreement algorithm.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
RSA with less than 1024 bit length Other unlisted algorithms	RSA (1024 bit or longer) for key exchange and protection DH RSA (1024 bit or longer) for digital signature	RSA (1024 bit or longer) for key exchange and protection DH	RSA (1024 bit or longer) for key exchange and protection DH	RSA (1024 bit or longer) for key exchange and protection DH	
Activities, Platforms, Operational Environments		All			

Table 3-14. Public Key Cryptography Implementations

3.6.4 Standards for Message Digest Algorithms

A variety of message digest algorithms exists. The two most widely used are the Secure Hash Algorithm - 1 (SHA-1), which is the NIST Standard for message hashing that is used in the NIST Digital Signature Standard (DSS), and the Message Digest-5 (MD5) which was developed by RSA laboratories and is used in many commercial products.

NIST Secure Hash Standard (SHA-1)

SHA-1 (also called just SHA) is the NSA designed, NIST issued federal standard for message digest functions. It is thought to be the strongest widely available message digest algorithm in common use. NIST Federal Information Processing Standard Publication 180-1 says about the

use of SHA-1, “This standard is applicable to all Federal departments and agencies for the protection of unclassified information that is not subject to Section 2315 of Title 10, United States Code, or Section 3502(2) of Title 44, United States Code. This standard is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required for Federal applications.”

Best Practices

When a choice of message digest algorithms is available (for example in the emerging S/MIME v3 e-mail security standard), SHA-1 should be selected in lieu of other available message digest algorithms.

Message Digest-5 (MD5)

MD5 was developed by RSA laboratories and is in widespread use in commercial products. Open literature cryptanalysis suggests MD5 may have weaknesses.

Best Practices

If no other choice is available in a commercial product, MD5 may be used. If a choice is available, the SHA-1 should be used.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Other unlisted algorithms	SHA-1 MD5	SHA-1	SHA-1	SHA-1	
Activities, Platforms, Operational Environments		All			

Table 3-15. Message Digest Algorithm Implementations

3.6.5 Digital Signatures

The two most widely used signature algorithms are the NIST Digital Signature Standard (DSS) and the RSA digital signature. DSS uses the SHA-1 digest algorithm (a government standard) and the El Gamal modified Diffie Hellman as the public key algorithm. RSA digital signature uses MD5 to calculate the message digest and RSA as the public key algorithm.

NIST Digital Signature Standard (DSS)

DSS is the NSA designed, NIST standard for digital signatures. The signature standard uses the SHA-1 hash algorithm and is thought to be stronger than methods based on weaker hash algorithms (for example, signatures based on MD-5). The NIST FIPS PUB 186 that defines the standard states:

"This standard is applicable to all Federal departments and agencies for the protection of unclassified information that is not subject to Section 2315 of Title 10, United States Code, or Section 3502(2) of Title 44, United States Code. This standard shall be used in designing and implementing public-key based signature systems which Federal departments and agencies operate or which are operated for them under contract. Adoption and use of this standard is available to private and commercial organizations."

Best Practices

When selecting a signature standard, Naval organizations should use the DSS whenever possible. This means it should be enabled in commercial products (for example in SSL for web transactions), should be specified when purchasing commercial products for Naval use, and should always be used when Navy and Marine Corps unique products are developed.

RSA Signatures

Digital signatures based on the RSA algorithm typically use the MD5 message digest algorithm with RSA public key algorithm although a growing list of applications use SHA-1 with RSA. This signature scheme is very widely used in commercial products owing to the long lag between the development of RSA digital signatures and the DSS.

Best Practices

Whenever possible, Navy and Marine Corps users should select products that use the DSS. However, in situations where DSS products are not yet available, Navy and Marine Corps users may use RSA signatures. If RSA is used, the SHA-1 message digest algorithm should be selected over the MD-5 message digest algorithm wherever possible. When more products provide implementations of the DSS, the use of RSA signatures will be disallowed.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Other unlisted algorithms	DSS RSA with SHA-1	DSS	DSS	DSS	
Activities, Platforms, Operational Environments		All			

Table 3-16. Digital Signature Implementations

3.7 References

DES

National Institute of Standards and Technology (NIST), "Data Encryption Standard" Federal Information Processing Standards Publication 46-2 (FIPS PUB 46-2), 30 December 1993

National Institute of Standards and Technology (NIST), “DES Modes of Operation” Federal Information Processing Standards Publication 81 (FIPS PUB 81), 2 December 1980

National Institute of Standards and Technology (NIST), “Security Requirements For Cryptographic Modules” Federal Information Processing Standards Publication 140-1 (FIPS PUB 140-1), 11 January 1994

DH

RSA Data Security, Inc., Public Key Cryptography Standard 3 (PKCS #3), Diffie-Hellman Key-Agreement Standard, Version 1.4, 1 November 1993, http://www.rsa.com/rsalabs/pubs/PKCS/ (23 May 1998)

DoD Wide Virus Detection Tool Site License

Space and Naval Warfare Systems Center (SPAWAR) PMW 161 Information Security (INFOSEC) web page: http://infosec.spawar.navy.mil (Internet) (23 May 1998) or http://infosec.navy.smil.mil (SIPRNET)

DSS

National Institute of Standards and Technology (NIST) “Digital Signature Standard (DSS)” Federal Information Processing Standards Publication (FIPS PUB) 186, 19 May 1994

Firewall Compatibility Requirements

Space and Naval Warfare Systems Command (SPAWAR) PMW-161 report,; “Firewall Services”, December 1996. ftp://infosec.navy.mil/pub/docs/navy/NSS/firewalls/fw_serv.doc

Cheswick, Bellovin; Firewalls and Internet Security; Addison-Wesley Publishing Company Reading MA; 1994

IPSEC

Metzger (Piermont) , Simpson (Daydreamer); “IP Authentication using Keyed MD5” (RFC 1828), August 1995. http://ds.internic.net/rfc/rfc1828.txt (23 May 1998)

Atkinson (Naval Research Lab); “IP Authentication Header” (RFC 1826) August 1995, ftp://ds.internic.net/rfc/rfc1826.txt (23 May 1998)

Atkinson (Naval Research Lab); “Security Architecture for the Internet Protocol” (RFC 1825). ftp://ds.internic.net/rfc/rfc1825.txt (23 May 1998)

Atkinson (Naval Research Lab) “IP Encapsulating Security Payload (ESP)” (RFC 1827). August 1995; ftp://ds.internic.net/rfc/rfc1827.txt (23 May 1998)

Karn (Qualcomm), Metzger (Piermont), Simpson (Daydreamer); “The ESP DES-CBC Transform” (RFC 1829) August 1995, ftp://ds.internic.net/rfc/rfc1829.txt (23 May 1998)

Krawczyk, Canetti (IBM), Bellare (UCSD); “HMAC: Keyed-Hashing for Message Authentication” (RFC 2104) February 1997, ftp://ds.internic.net/rfc/rfc2104.txt (23 May 1998)

Oehler (NSA), Glenn (NIST); “HMAC-MD5 IP Authentication with Replay Prevention” (RFC 2085). February 1997, ftp://ds.internic.net/rfc/rfc2085.txt (23 May 1998)

Maughan, Schertler, Schneider, Turner; “Internet Security Association and Key Management Protocol.” 10 March 1998, ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-09.txt (23 May 1998)

Orman (Univ. of Arizona); “The OAKLEY Key Determination Protocol.” 27 April 1998, ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsec-oakley-02.txt (23 May 1998)

The resolution of ISAKMP with Oakley. (ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-oakley-05.txt)

MD5

Rivest (MIT and RSA Data Security Inc.); “The MD5 Message-Digest Algorithm” (RFC1321) April 1992. http://ds.internic.net/rfc/rfc1321.txt (23 May 1998)

Metzger (Piermont) , Simpson (Daydreamer); “IP Authentication using Keyed MD5” (RFC 1828), August 1995. http://ds.internic.net/rfc/rfc1828.txt (23 May 1998)

Operating System Security

Department of Defense; “Department of Defense Trusted Computer System Evaluation Criteria” (The Orange Book), DoD 5200.28-STD, December 1985.

Space and Naval Warfare Systems Command; “Secure Windows NT Installation and Configuration Guide”, SPAWAR PMW-161 Report, November 1997. ftp://infosec.navy.mil/pub/docs/navy/NT-SECURITY/navynt.zip (23 May 1998)

Space and Naval Warfare Systems Center (SPAWAR) PMW 161 Information Security (INFOSEC) web page: Various document on best commercial practices in UNIX security. ftp://infosec.navy.mil/pub/docs/unix/ (23 May 1998)

RSA Public Key Cryptography

RSA Data Security Inc., “Public Key Cryptography Standard 1 (PKCS #1),” 1998, http://www.rsa.com/rsalabs/pubs/PKCS/ (23 May 1998)

RSA Data Security, Inc., “Public Key Cryptography Standard 7 (PKCS #7), Cryptographic Message Syntax Standard”, 1998, http://www.rsa.com/rsalabs/pubs/PKCS/ (23 May 1998)

SHA-1

National Institute of Standards and Technology (NIST), “Secure Hash Standard” FIPS PUB 180-1, 17 April 1995, http://csrc.nist.gov/fips/ (23 May 1998)

S/KEY

Haller (Bellcore), “The S/KEY One-Time Password System” (RFC 1760), February 1995. http://www.cis.ohio-state.edu/rfc/rfc1760.txt (23 May 1998)

S/MIME

Blake, Ramsdell (Worldtalk); “S/MIME Version 2 Message Specification”(Internet Draft), 4 May 1998, http://www.imc.org/draft-ietf-smime-msg (23 May 1998)

Blake, Ramsdell (Worldtalk) “S/MIME Version 2 Certificate Handling” (Internet Draft), 4 May 1998, http://www.imc.org/draft-ietf-smime-cert (23 May 1998)

SSL

Frier, Karlton (Netscape), Kocher (independent); “The SSL Protocol, Version 3.0” (Internet Draft); 18 November 1996; http://home.netscape.com/eng/ssl3/draft302.txt (23 May 1998)

Triple DES (3DES)

4. Facility and Environmental Requirements

This chapter includes mechanical, electrical, and cable plant standards and guidance for shipboard and shore/base environments, as well as ground combat and naval aircraft environments. The relationship of this chapter with the ITSG is shown in Figure 4-1.

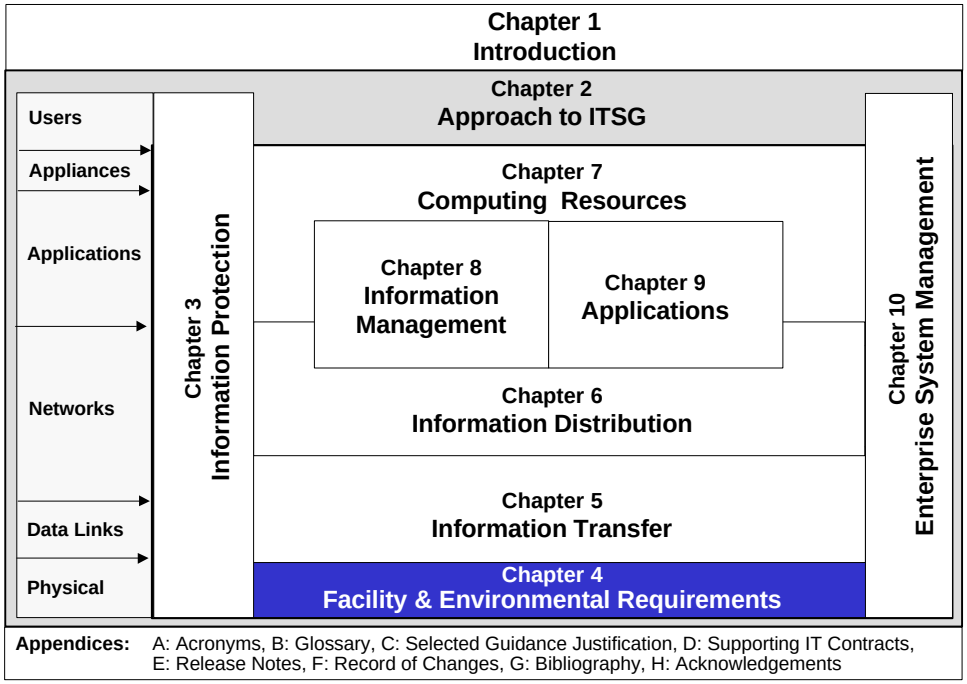


Figure 4-1. ITSG Document Map Highlighting Chapter 4, Facility and Environmental Requirements

4.1 Overview

The purpose of this chapter is to provide facility and environmental requirements for commercial off-the-shelf (COTS) Information technology (IT) components. Often, information processing equipment such as personal computers, are considered to be small electrical appliances that do not require additional considerations above those already present for the facility. Experience has shown that commercial off-the-shelf (COTS) equipment can survive and reliably operate within enclosed air-conditioned spaces of shore-based facilities and Navy ships provided that some reasonable and practical installation guidelines are followed. However, the number of “small” computers can add up and place a considerable load on the facility, particularly in the shipboard environment. Standards and specifications are well established for cabling, fire prevention, electrical safety, cooling, and physical security.

The goal of this chapter is to provide a complete and comprehensive set of facility specifications pertaining to IT implementation. These facility specifications are distributed among many different references pertaining to different platforms, operating environments, and physical technology. The current version of the ITSG does not exhaustively meet this goal, however, it does provide a placeholder to contain that information in the future.

4.2 Site Security

Classified site security requirements for facilities is provided in DoD 5220.22-M dated January 95, National Industrial Security Program Operating Manual (NISPOM).

4.3 Cable Plant

The cable plant includes copper cable, fiber optic cable, and wireless RF. Wireless optical devices currently satisfy only special-purpose requirements and are beyond the scope of the ITSG.

Best Practices

Fiber optic cable is the solid media preferred for its current high-capacity (100's of Mbps), future bandwidth potential (Gbps to Tbps), reliability, reduced susceptibility to Electromagnetic Interference (EMI), and security. (Although fiber cannot be made completely secure without encryption or proper physical protection, it cannot be "tapped" without physical manipulation.)

Fiber optic cable is required to support voice and high speed data. Fiber optic cable is recommended in other areas where feasible. If cost limits its use, then fiber optic cable should be run at least in the backbone of the network and to major junction points (telephone closets, for example). A mix of 62.5µm core/125µm cladding multimode and 8µm core/125µm cladding single-mode fiber should be pulled in jacketed bundles, terminated and tested. The cost avoidance of installing additional single-mode cable is relatively low compared to the future benefits it presents.

Copper cabling should be avoided in the backbone because it has inherently low bandwidth over significant distance. If copper is unavoidable, it should be limited to areas which can be easily, and inexpensively rewired with fiber when appropriate. If copper is used, select only properly-terminated and tested Category 5 ("Cat 5") cable for cable from the telecommunications closet to the desktop. (Unshielded Twisted Pair (UTP) Cat 5 is *the* copper standard for data rates up to 155 Mbps.) Thin-wire coax, thick-wire coax, RS-232/422, Category 3 and "telephone" wire should be avoided — the minor cost savings is not usually justifiable because of limited data rates and degraded interoperability. (Allowable exceptions are recognized when linking distant, or otherwise limited-access areas, which are already wired.)

Table 4-1 and Table 4-2 provide recommended implementations.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Coaxial Cable 10BASE5 (ThickNet) 10BASE2 (ThinNet) Thick Net Shielded Twisted Pair RS-232/422 Cat-3 Cable	MIL-F-49291 MIL-C085045 Air Blown Fiber (ABF) Zip Cord for Drop Cables UTP Cat-5 for Drop Cables after testing	MIL-F-49291 MIL-C085045 Air Blown Fiber (ABF) Zip Cord for Drop Cables UTP Cat-5 for Drop Cables after testing	MIL-F-49291 MIL-C085045 Air Blown Fiber (ABF) Zip Cord for Drop Cables UTP Cat-5 for Drop Cables after testing	MIL-F-49291 MIL-C085045 Air Blown Fiber (ABF) Zip Cord for Drop Cables UTP Cat-5 for Drop Cables after testing	Wireless IEEE 802.11
Activities, Platforms, Operational Environments		Ships			

Table 4-1. Cable Media Recommended Implementations for Ships

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Coaxial Cable 10BASE5 (ThickNet) 10BASE2 (ThinNet) Thick Net Shielded Twisted Pair RS-232/422 Cat-3 Cable	Mix 62.5 um core/125um clad multi-mode with 8um core/125um clad single-mode fiber Air Blown Fiber (ABF) Zip Cord for Drop Cables UTP Cat-5 for Drop Cables after testing	Mix 62.5 um core/125um clad multi-mode with 8um core/125um clad single-mode fiber Air Blown Fiber (ABF) Zip Cord for Drop Cables UTP Cat-5 for Drop Cables after testing	Mix 62.5 um core/125um clad multi-mode with 8um core/125um clad single-mode fiber Air Blown Fiber (ABF) Zip Cord for Drop Cables UTP Cat-5 for Drop Cables after testing	Mix 62.5 um core/125um clad multi-mode with 8um core/125um clad single-mode fiber Air Blown Fiber (ABF) Zip Cord for Drop Cables UTP Cat-5 for Drop Cables after testing	Wireless IEEE 802.11
Activities, Platforms, Operational Environments		Shore, ITSCs			

Table 4-2. Cable Media Recommended Implementations for Shore and ITSC Use

4.3.1 Definitions

4.3.1.1 Trunk Cable

A trunk cable is a cable that connects two main interconnection boxes or patch panels. It is used to provide connectivity between the service areas of the cable plant.

4.3.1.2 Local Cable

A local cable is a cable that connects a main interconnection box or patch panel to user system equipment or a local breakout box.

4.3.1.3 System Specific Cable

A system specific cable directly connects two pieces of user system equipment, independent of the cable plant. A system specific cable is typically used to connect equipment within the same service area of the cable plant.

4.3.1.4 Drop Cable

A drop cable is a system specific cable between a ready movable piece of user system equipment, such as a PC or printer, and the local breakout box in the area. A drop cable is not considered to be part of the cable plant.

4.3.2 Media

4.3.2.1 Fiber Optic Cable

Fiber optic cable is the preferred media for all network applications due to its growth potential. (In shipboard and other high Electromagnetic Interference (EMI) environments, fiber optic cable is critical in eliminating the effects of noise.) The backbone network must use fiber optic cabling, as part of the Fiber Optic Cable Plant (FOCP) — twisted pair (shielded or unshielded) or coaxial cable should not be used. Where possible, multimode graded index fiber with a 62.5 micrometer (µm) core/125µm cladding should be used. Due to the low relative marginal cost, single-mode fiber (8µm core/125µm cladding) should be provided in at least the backbone FOCP and preferably to major junction points.

Multimode fiber (62.5µm) is easier to terminate and test, especially in the field. However, there are distance and bandwidth limitations that cannot be overcome and single-mode fiber must be used. (Multimode fiber can support rates of up to 155 Megabits Per Second (Mb-ps) at distances up to 2 kilometers (km). It can only support 622 Mbps for hundreds of feet. Single-mode fiber (8µm), however, can easily support units of Gigabits Per Second (Gbps) at up to 30 kms. Further, it can support multiple wavelengths, each operating at units of Gbps. Thus today's single-mode fiber can support tens of Gbps for tens of kilometers. Laboratory tests have shown this limit to be at least 2 orders of magnitude higher, namely Terabits Per Second (Tbps).

4.3.2.1.1 Testing Fiber Cable for Kink Susceptibility

Recent purchase of fiber optic cable has demonstrated a susceptibility to kinking that results in excessive optical loss. Contact Naval Sea Systems Command (NAVSEA) 03J for a test procedure that can detect this potential problem while the cable is still on the reel.

4.3.2.2 Unshielded Twisted Pair (UTP)

Category 5 UTP cable may be used only for the cabling between the appliance and the network edge device or between the workstation and other network equipment under certain conditions. Shielded Twisted Pair (STP) cable should not be used. The following factors should be taken into consideration when using Category 5 UTP cable:

- Mission criticality of the application (The UTP copper cable may exhibit a lower availability than fiber due to EMI problems.)
- Bandwidth or signaling rate (UTP may be used for short runs of 100BaseT, but should not be used at higher data rates or for long runs.)
- Security level (UTP is easy to tap if not run in conduit.)
- Length of cable run (UTP should be limited to intra-compartment runs.)
- Installation factors (UTP requires exceptional care during installation, and should be thoroughly tested.)
- Environmental factors
- EMI (UTP is subject to interference from radar and nearby high-powered equipment.)

In shipboard environments, UTP cable should meet the flammability, smoke, acid gas generation, halogen content, and toxicity index requirements noted in the previous section for fiber cable. Further, UTP should be limited in mission critical systems to non-critical components due to EMI, shock and vibrations (commercial RJ-45 plastic connectors for UTP are not designed to withstand significant shock loads and may crack or disconnect under long-term vibration conditions).

4.3.2.3 Legacy Copper-Media Networks

For installations with copper-based legacy systems, it is recommended that those systems be selectively upgraded to fully integrate users of the backbone network based on capability requirements and funding availability. In the case of remote runs, particularly on large shore installations, legacy copper may not be replaced for a significant period of time, if ever. Alternate technologies, such as cable modems or Digital Subscriber Line (DSL), may be the only mechanism for providing high-bandwidth access. (A relevant example would be a guard shack located many miles from the nearest network access point. Should this outpost need multiple Mbps for a video circuit (camera or monitor), an existing POTS line may be all that is ever available. In this case, a DSL modem may suffice.) Again, it is strongly preferred that all copper infrastructure be replaced with fiber — even if it takes years.

In shipboard environments where the ship's decommissioning schedule, upgrade funding availability, or system requirements cannot support the decision to upgrade the system, connectivity to the ship's backbone network can be accomplished at either the backbone or workgroup switch, providing that the legacy network protocols can be supported by those devices. In such a configuration, the backbone network switch acts as a gateway between the legacy system and the rest of the backbone. If some limited funding for system upgrade is available, and such upgrades suit the needs of the ship, a lower cost interim upgrade would be to replace the legacy copper links with fiber optic links, and integrate those links into the ship's FOCP. This interim physical integration will simplify the further upgrade from a separate legacy system to an integrated network application.

4.3.2.4 Shipboard Environment

In shipboard environments, the fiber should meet the requirements of MIL-F-49291. The fiber optic cables should meet the requirements of MIL-C-85045 (including, but not limited to, flammability, smoke, acid gas generation, halogen content, and toxicity index). A requirement for the use of Air Blown Fiber (ABF) as an alternative installation technique for fiber optic cabling in ships is under development. Specific requirements for ABF use will be provided at a future date.

4.3.2.5 Shore/Base Environment

In shore and base environments, the fiber optic cable's outer jacket composition must comply with National Fire Protection Association (NFPA) standards that address use within plenums. Electrical code must be followed when non-dielectric-strength members are used (e.g., for additional support or rodent protection.) Building interior backbones should nominally consist of 24 multi-mode fibers and 12 single-mode fibers with the actual numbers determined by the local command. For building and base exterior backbones, runs of 2 km or less will use composite cable consisting of 8 multi-mode fibers and 4 single-mode fibers. Runs greater than 2 km should consist of single-mode fibers; the number to be determined by the local command or the ITSC. For tough or long cable pulls, 200-Kilo-Pounds-per-Square-Inch (KPSI)-rated cable is recommended, otherwise 50-KPSI-rated cable is acceptable. Area installations will use dielectric-strength members to provide lightning protection. All runs will be supported to prevent excessive sagging.

4.3.2.6 Pier and Mooring Stations

A 12-fiber composite cable and covered connectors should be run from the pier junction box to each pier berth. The outer jacket is ruggedized and weatherproof. Umbilical cables will be used to connect the pier mooring station to the ship junction box. The cable itself should be a composite cable consisting of 8 multi-mode fibers and 4 single-mode fibers per Section 4.3.2.1.

4.3.2.6.1 Pier Trunk Cable

The pier trunk cable shall have a heavy duty PVC outer jacket designed for direct burial, underground duct, steam tunnel, or aerial-lashed installation. It shall be designed for water blocking per EIA/TIA-455-82B and operating temperatures from -40C to +85C.

4.3.2.6.2 Umbilical Cable

The umbilical cable shall be suitable for tactical field use in severe environmental conditions. There are two polyurethane outer jackets that should be separated by an E-glass yarn for maximum flexibility. The outer jacketing shall be designed for maximum abrasion, cut, and chemical resistance over a wide temperature range (-55C to +85C). Internal construction should have two separate layers of Kevlar for maximum crush resistance and resilience (DOD-STD-1678).

4.3.2.6.3 Shipboard Trunk Cable

The shipboard cable connecting the mooring stations to the junction box in the radio room should have the same outer jacketing construction as the umbilical cable except that there is a single outer jacket. The jacketing shall be UV inhibited, flame retardant, and moisture/fungus resistant. The internal construction shall have sub-cable jacketing that separates the internal fibers into pair groupings.

4.3.3 Patch Panels, Interconnection Boxes and Connectors

Recommended Implementations

The recommended implementations for the patch panels, interconnection boxes, and connectors is provided in Table 4-3 and Table 4-4 for ship and shore implementations respectively.

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
MIC fiber connectors	MIL-I-24728 for interconnection boxes MIL-C-83522/16 ST connector for multimode fiber FOPC connector for single mode fiber RJ-45 for UTP cable	MIL-I-24728 for interconnection boxes MIL-C-83522/16 ST connector for multimode fiber FOPC connector for single mode fiber RJ-45 for UTP cable	MIL-I-24728 for interconnection boxes MIL-C-83522/16 ST connector for multimode fiber FOPC connector for single mode fiber RJ-45 for UTP cable	MIL-I-24728 for interconnection boxes MIL-C-83522/16 ST connector for multimode fiber FOPC connector for single mode fiber RJ-45 for UTP cable	SC connector for multimode fiber
Activities, Platforms, Operational Environments		Shipboard			

Table 4-3. Patch Panels, Interconnection Boxes and Connectors Recommended Implementation for Shipboard Use

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
MIC fiber connectors ST fiber connectors.	SC connector for multimode fiber FOPC connector for single mode fiber RJ-45 for UTP cable	SC connector for multimode fiber FOPC connector for single mode fiber RJ-45 for UTP cable	SC connector for multimode fiber FOPC connector for single mode fiber RJ-45 for UTP cable	SC connector for multimode fiber FOPC connector for single mode fiber RJ-45 for UTP cable	
Activities, Platforms, Operational Environments		Shore and ITSC			

Table 4-4. Patch Panels, Interconnection Boxes and Connectors Recommended Implementation for Shore and Base Use

4.3.3.1 FOCP Interconnection Boxes

FOCP interconnection boxes and patch panels should hold a minimum of 48 connector pairs. Interconnection boxes should be sized to accommodate all of the fibers (allocated, spare, and growth) that enter the box.

4.3.3.2 Local Breakout Boxes

Local breakout boxes may be used to provide additional flexibility in locating workstations or easily moved equipment. The interconnection box should completely enclose the fiber

terminations. Local breakout boxes should not be used as a substitute for rack-mounted patch panels for the interconnection of rack-mounted equipment.

4.3.3.3 Location of Tx-Rx Pairs and Optical Crossover

In FOCP Interconnection Boxes, local breakout boxes, and in rack-mounted patch panels, the pair of ST connectors associated with one full-duplex optical circuit should be located in a vertical line, one above the other, with the transmit (Tx) connector above the receive (Rx) connector. In a complete optical link, there must be one (or an odd number of) crossovers in order to connect the optical transmitter at one end to the optical receiver at the other end, and vice versa.

4.3.3.4 Shipboard Environment

In shipboard environments, interconnection boxes should meet the requirements of MIL-I-24728. Breakout boxes should be in accordance with MIL-I-24728/4 or /5, and should be mounted within the same compartment as the equipment they serve

4.3.3.5 Shore/Base Environment

In shore and base environments, all cabling will be terminated in lockable fiber optic patch panels. Patch panels will have splice trays or allowances for splices for the single-mode fiber. A minimum of 25 foot service loop will be used at each end of the cable for interior building backbones and 50 foot service loop for exterior building/base backbones. Tight buffered construction will be used and the cables should be supported. For exterior/base backbones, tight buffered construction will be used unless outer cable diameter or high moisture environments required use of gel-filled cable. All gel-filled installations will use the proper blocking kits to prevent gel creep. The cables should be supported to prevent excessive tension or compression.

4.3.3.6 Pier and Mooring Stations

On board the ship, ruggedized, weatherproof fiber optic junction boxes with weatherproof fiber optic patch panels are required at both the port and starboard mooring stations. Submarines will have one junction box with two connections. On the pier, ruggedized weatherproof fiber optic junction boxes with patch panel uplinked to the base area network and downlinked to each pier berth are required.

4.3.4 Connectors

4.3.4.1 Fiber Optic Cable

4.3.4.1.1 ST-type

ST-type connectors were, until recently, the standard for all multimode connections. In commercial applications, SC is rapidly becoming the standard. It is becoming hard to find host network interface cards with ST connectors.

4.3.4.1.2 SC-type

SC-type connectors are becoming the industry standard for both host network interface cards and backbone connections. While this is acceptable for multi-mode fiber, it has debatable merit for single-mode fiber. (Pros: more common connector, easier to insert/remove; Cons: can more easily

confuse multi-mode with single-mode fiber, if single-mode transmitter accidentally plugged into multi-mode receiver, the receiver could be permanently damaged.) The choice for shore-based systems is not critical.

4.3.4.1.3 FCPC-type

FCPC-type connectors are the standard for single-mode fiber. Many equipment vendors, however, are beginning to use SC-type connectors. Because the risk of accidentally switching multi-mode and single-mode connections exists when the same connector is used for both, it is recommended that FCPC-type be used for single-mode fiber (see discussion in the previous paragraph).

4.3.4.1.4 MIC-type

MIC-type connectors are not recommended for use within the backbone network. However, if MIC-type connectors are the only available option, it is recommended that a MIC-ST jumper cable be fabricated to allow the MIC connector at the equipment interface, but with an ST connector for connection to the FOCP or rack-mounted patch panel. MIC connectors should not be used within FOCP interconnection boxes.

4.3.4.1.5 Heavy-Duty Multiple Terminus

Heavy-duty multiple terminus connectors are recommended for equipment interfaces that require a rugged interface that is easily disconnected and reconnected. These connectors should be in accordance with MIL-C-28876, except for ship-to-shore pier connections which will comply with requirements stated in section 4.3.4.5.

4.3.4.1.6 Mechanical Splice

Mechanical splices are recommended only for those applications requiring higher optical performance than is available with ST-type connectors. Mechanical splices should meet the requirements of MIL-S-24623. Mechanical splices may be used in interconnection boxes, and may also be used inside rack-mounted patch panels where needed for higher optical performance.

4.3.4.2 Copper Cable

4.3.4.2.1 RJ-45 Connectors

Category 5 cable specifications limit the connector type to RJ-45. However there are a number of pin-out standards from which to choose. Because ISDN also specifies the use of RJ-45, the ISDN pin-out specification will be used: ANSI/EIA/TIA-568-1991 Standard, Commercial Building Telecommunications Wiring. This standard defines pin-outs as shown in Figure 4-2. This variant is designated EIA/TIA T568A (also called ISDN, previously called EIA).

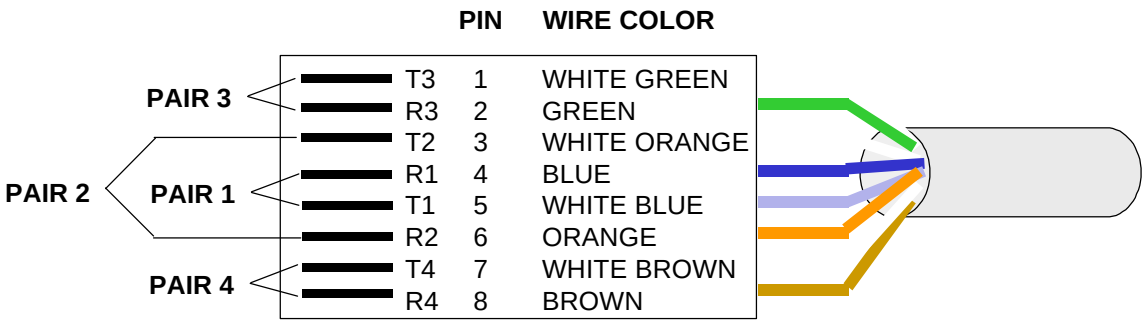


Figure 4-2. RJ-45 Pin Specifications for T-568A

4.3.4.3 Shipboard Environment

In shipboard environments, ST-type connectors are recommended for all light-duty multi-mode fiber applications. For FOCP connections inside interconnection boxes, the connectors should be in accordance with MIL-C-83522/16. ST-type connectors may be used as the interface to equipment if sufficient cable strain-relief and protection are provided. Failure to provide sufficient strain relief and protection will result in connector breakage or failure.

Until such time as SC-type connectors are evaluated against shock, vibration and wear, they are not recommended for use within the backbone network. However, if SC-type connectors are the only available option associated with the network equipment, it is recommended that an SC-ST jumper cable be fabricated to allow the SC connector at the equipment interface with an ST connector for connection to the FOCP or the rack-mounted patch panel. SC connectors should not be used within FOCP interconnection boxes.

4.3.4.4 Shore/Base Environment

In shore/base environments, SC-style connectors are recommended. Duplex connectors are recommended at the terminal ends of the workgroup and network device ends. Patch panel jumpers should be simplex to allow for rerouting of separate cables. Ceramic ferrules are recommended for superior loss and polishing characteristics. Wall-mounted faceplates are recommended. Zip cord is recommended for the drop cables from the wall faceplate to the appliance. UTP with standard RJ-45 connector is acceptable as well.

4.3.4.5 Pier and Mooring Stations

A ruggedized, weatherproof, 12-pin fiber optic connector will be used to connect the pier berth to the umbilical and the umbilical to the ship mooring station junction box. The umbilical will also be used to connect between ship junction boxes for ships nested outboard. The connector itself should be hermaphroditic (“genderless”) for greater simplicity over male-female connectors. The hermaphroditic connector should be a 12 pin connector consisting of 8 pins multi-mode optical fiber and 4 pins single mode optical fiber. The termini should be MIL-T-29504/14 & /15.

4.3.5 Topology, Security & Integrated Cabling

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	Mesh Topology MIL-STD-2042 for ships cabling MIL-HDBK-2051 for ships ANSI/TIA/EIA 568A, 569 for shore	Mesh Topology MIL-STD-2042 for ships cabling MIL-HDBK-2051 for ships ANSI/TIA/EIA 568A, 569 for shore	Mesh Topology MIL-STD-2042 for ships cabling MIL-HDBK-2051 for ships ANSI/TIA/EIA 568A, 569 for shore	Mesh Topology MIL-STD-2042 for ships cabling MIL-HDBK-2051 for ships ANSI/TIA/EIA 568A, 569 for shore	
Activities, Platforms, Operational Environments		All unless otherwise noted.			

Table 4-5. Topology, Security, Cable Integration Recommended Implementations

4.3.5.1 Basic Topology

The recommended physical topology is a mesh, as opposed to a ring or star configuration. If a logical ring or star topology is required for near-term cost reasons, the physical mesh cable plant infrastructure can be configured to provide the required logical topology. The mesh physical architecture will support the future expansion or upgrade to a full mesh logical topology.

4.3.5.2 Network Node Locations

Node locations should be selected based on the concentrations of current and planned network users. Nodes should be located in secure areas, to preclude unauthorized access to the equipment. Nodes should also be located in temperature controlled compartments, to optimize equipment reliability. Note that there is a trade-off between the number of nodes and the total quantity of local cable required to connect users. These two parameters should be considered in conjunction with the system requirements for survivability when determining the appropriate number of nodes.

In shipboard environments, users should be connected to nodes within the same fire zone for survivability. Also, the number of nodes installed should be selected to provide maximum coverage of the ship's fire zones, while minimizing the total network cost.

4.3.5.3 Patch Panel And Interconnection Box Locations

Main interconnection boxes or patch panels should be collocated with the network nodes. For maximum installation and connection flexibility, it is recommended that the patch panels be installed in the same rack as the network node equipment. These rack-mounted patch panels can also be used to provide a convenient means of interconnecting equipment within the same rack, and to provide a simplified disconnect point in the event that racks must be moved.

In shipboard environments, interconnection boxes should be in accordance with MIL-I-24728 and be bulkhead mounted. For racks containing connection-intensive network devices, the use of a rack-mounted patch panel should be considered to serve as the interconnection box for that zone.

4.3.5.4 Trunk Cable Routing

In general, trunk cables should be routed along diverse physical paths to ensure a survivable FOCP. The degree of redundant/fail-over equipment is cost-driven but with a proper FOCP mesh, outages can be quickly restored using alternate cable paths.

In shipboard environments, trunk cables should be routed to provide survivable signal paths between interconnection boxes in accordance with the requirements of MIL-STD-2042. In general, each trunk cable should have an identical redundant cable following a separate route between the two interconnection boxes. The separation recommendations are to be followed for distributed systems, as defined in Section 072 of the applicable ship specification. In addition, the cables should be routed on opposite sides of the ship, with at least two decks separating them vertically. If possible, it is desirable to have one of the runs located primarily below the damage control deck, and the other above the damage control deck, but this must be factored along with technical and cost feasibility guidance.

4.3.5.5 Local Cable Distribution

In shipboard environments, local cables should be routed in accordance with the requirements of MIL-STD-2042. If a single user has multiple local cables for redundancy or survivability, those local cables should be routed to two different interconnection boxes, and should be separated within 60 feet of the equipment.

4.3.5.6 Network Fiber Allocations

4.3.5.6.1 Inter-node

Fibers should be allocated for all inter-node connections. The level of inter-node connectivity should be determined based on current technical requirements, future projections of requirements, and overall program cost constraints. In general, it is desirable to include sufficient fiber in the FOCP to allow for full inter-node connectivity in a mesh topology. Any interim logical configurations, such as rings or stars, should also be considered when determining fiber requirements.

4.3.5.6.2 Redundancy

Redundant fibers in survivable separated trunk cables should be provided for each active and spare user system fiber. This is particularly critical in shipboard environments.

4.3.5.6.3 Spares

Spare fibers should be provided on a 100% basis; that is, each actively used fiber should have an assigned spare. This is particularly critical in shipboard environments.

4.3.6 Cable Security

In general, the requirements of National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST 2/95, RED/BLACK Installation Guidance apply. Further explanation and recommendations on security related topics are provided below.

4.3.6.1 Use of Separate RED and BLACK Cables

Per the TEMPEST guidelines, separate multifiber cables should be used for RED and BLACK systems. However, these cables may be in the same trunk group.

4.3.6.2 Use of Conduit for RED Cables

Encasing RED cables in conduit does not provide an additional level of security commensurate with the associated costs (including weight and volume impact on the ship).

4.3.6.3 Locking Interconnection Boxes

Interconnection boxes containing RED fibers should be locked, or located inside a secured space. Locating the boxes in a secure space is the preferred option.

4.3.6.4 Separation of RED and BLACK Fibers Inside an Interconnection Box

For maximum security, separate RED and BLACK interconnection boxes should be used. If separate boxes are cost prohibitive, an alternative is to use separate patch panels in the same interconnection box for RED and BLACK terminations. If only one patch panel is used, RED and BLACK fibers should be segregated to prevent mis-connections.

4.3.6.5 Connector Selection

The TEMPEST guidelines recommend using incompatible connector types for RED and BLACK connections. For multifiber (heavy-duty) connectors, this can be accomplished by specifying an alternate keying arrangement for RED connectors. Within interconnection boxes, there are two connection options -- the light-duty, single-fiber connector and the rotary mechanical splice. The rotary splice is a high performance termination that is more expensive and best suited to specific applications requiring very low insertion loss terminations. Therefore, it is recommended that the selection of termination type inside the interconnection box should be governed by the system's optical performance requirements, rather than security classification level. In addition, the practice of using light-duty connectors with a different color boot is recommended as a way to distinguish RED versus BLACK connections.

4.3.6.6 Labeling and Marking

The current General Specification (GENSPEC) labeling and marking conventions for cables and fibers do not have any provisions for handling RED versus BLACK designations or Transmit versus Receive ends of a fiber. It is recommended that, upon installation, RED fibers be labeled as such using an extra heat shrink sleeve. These labels should only be added after the cable jacket is stripped off exposing the individual OFCCs. Note that all fibers in the RED cables should be labeled as such, including spare and growth fibers, since mixing RED and BLACK fibers in the

same cables is not permitted. It is further recommended that the transmitting end of a fiber (the end from which light exits if the connection is opened) be labeled “T” or “Tx” and the receiving end be labeled “R” or “Rx”.

4.3.6.7 Sharing of Trunk Fibers

Each fiber in a trunk cable is reserved for one unidirectional optical communication link for one transmitter/receiver pair. No near-term plans are in place to permit wavelength division multiplexing, or to put multiple light signals down the same fiber. The fibers within a particular trunk cable may be allocated to different equipment within the same system, or even different systems, subject to the information security provisions described above. However, each fiber provides a completely isolated communication path from all the other fibers in the cable.

4.3.6.8 Sharing of Interconnection Boxes

Multiple user systems will share the same fiber optic interconnection boxes, again subject to the aforementioned security requirements.

4.3.7 Cable Plant Integration Guidance

4.3.7.1 Use Of Existing FOCP

When an installation already has an FOCP, a new network should make maximum use of the existing FOCP. At a minimum, every attempt should be made to make use of growth capacity within the FOCP interconnection boxes or patch panels, even if additional cabling must be installed to support the network connectivity requirements.

4.3.7.2 Shipboard Implementation Guidance

The shipboard cable plant provides the physical layer fiber optic connectivity for networks and other user systems on the ship. The fiber optic cable plant (FOCP) supports multiple ship service areas. Each service area is provided with one or more fiber optic interconnection boxes to allow cable plant access for the user equipment. From the interconnection box, fiber optic connectivity to other service areas is provided through redundant, survivable separated fiber optic trunk cables. The design guidance of MIL-HDBK-2051 and MIL-STD-2052A, as well as the installation requirements of MIL-STD-2042, applies to all ship fiber optic cable plants.

4.3.7.3 Shore Based Implementation Guidance

ANSI/TIA/EIA 568A,569 are the core of a popular family of commercial cabling standards for building and campus telecommunications infrastructure. These standards support telecommunications applications for current and emerging voice, video and data applications. Through active participation and consensus, North American telecommunications manufacturers, designers, consultants, and commercial and government users develop the standards. (Although the primary focus of this group is the North American marketplace, members provide liaison with international standards bodies and also serve as representatives in the United States Technical Advisory Group and Canadian Standards Association.) In addition to these standards, Type I security requirements are established for conduit and/or alarms.

4.3.8 Cable Plant Management

Requirements

It is recommended that all installations have a reliable and accurate cable plant management system. The system shall be integrated into the enterprise management system (Chapter 10). The Web-Based Enterprise Management (WBEM) specification provides guidelines for integration.

A number of cable plant management packages exist that meet the DON requirements. In shipboard environments in which damage control is part of the routine, it is especially critical to have a robust system. The following is recommended for this environment and encouraged for all environments.

Physical and Logical Network View. Users should be able to examine the network physical connections from a high-level topological view down to the fiber and port level via a 3-D graphical representation of the networking environment. Users should also be able to examine the logical connections of the network. The software should display multiple ship decks with Naval isometric format in a single window viewport. It should display in a single window viewport the fiber optics backbone across multiple ship decks. Classified and unclassified networks must be displayed in different colors. Also, individual user systems and their cables must be displayed in different colors.

System Requirements. The software should be built upon advanced COTS Open-GL 3D graphics engine, Relational Data Base Management Systems (RDBMS), and trouble-ticketing software. It should be able to handle DON specific cable plant requirements. It should be able to import multiple ship electronic drawings and compartmentation booklets, and integrate these into a single Naval isometric drawing format. The RDBMS software should provide the users with a robust database management tool and report generation capability. The integrated system should enable recognition of components and cable connections across the individual COTS-based software products (database, troubleticketing, network management tool, cable management software) that comprise the integrated product.

Network Equipment Asset Accounting. The software should provide cable asset management, complete with defect reporting and asset tracking and reporting functionality.

Trace Path Function. The software should provide a single window viewport and “any-to-any" cable trace path capability – from any active network components and passive cable plant components to any other active network components and passive cable plant components. This capability will allow users to dissect the connectivity of the network components and to reroute connections from the shortest path (if that connection is "down") to the next shortest spare/redundant path.

Change Management. The software should allow users to manipulate (add, modify, describe, delete) network components. These components consist of communications devices, switching hubs, ATM switches, junction boxes (Navy-specific FOICBs), patch panels, splice-trays, pig-tails, media converters, outlets, trunks, fiber cables and copper cables. The system must address fiber optics and copper cables and connectors.

Dynamic Routing And Cable Tracking. The software should provide program recommendations to allow network managers to re-route communication paths dynamically

and quickly when existing paths are damaged or destroyed. Thus, under the most severe battle conditions, the cable plant management capabilities will provide the ship with continued communications as long as alternative paths are available for re-routing purposes.

Fault Reporting. The system administrator should be able to detect a fault, to determine the location of the physical problem, and to issue a maintenance request in one unbroken sequence.

Security. The software should provide at least three levels of security login: read-only, integrator, and system administrator.

Help Function. The software should offer extensive online help complete with a glossary that defines the terms used in the program.

Specifications that support these functions are addressed in Chapter 10. Remote Network Monitoring version 2 (RMON2) and the Simple Network Management Protocol (SNMP) are the two current specifications.

Best Practices

Use Simple Network Management Protocol (SNMP) version 1 and Remote Network Monitoring Protocol version 2 (RMON 2) to manage IP networks and integrate the network management system into the DON enterprise management system.

4.4 Shipboard Facility Requirements

4.4.1 Racks

Shipboard networking equipment should never be installed by setting them upon desks, tables, filing cabinets, etc. Small equipment can be bulkhead-mounted or hung from the overhead; however, the preferable technique for shipboard installation of COTS networking equipment is in racks.

Suitable racks can be obtained from a number of vendors. However, heavy duty, industrial grade or ruggedized racks should be used, not lightweight racks intended for office environments.

Standard rack widths are 19” and 24”. Nearly all COTS networking equipment is designed to fit into 19” wide racks. (Note that these are mounting widths; the overall external width of a 19” rack is about 24”, and the outside width of a 24” rack is about 30”.)

Standard 19” racks come in several depths, typically 17”, 24”, 29” and 36”. When deciding on the depth of a rack, remember to allow enough depth for recessing equipment that have front-access cabling, and to allow air exhaust space for equipment with rear-facing fans. Many pieces of networking equipment have modular assemblies that are removed from the front, and the cables attach to these assemblies from the front. This requires that the unit be recessed at least 4” to allow a reasonable cable bending radius. (For units that have rear-accessible modules, it is often desirable to mount them in backwards for easier access to removable modules.)

If there is sufficient space in the shipboard compartment to mount the racks away from the bulkhead for both front and rear access, a sufficiently deep rack will permit electronics units and fiber patch panels to be placed back-to-back at the same vertical level within the rack.

Consider cable entry when ordering racks. If the rack is to be located on a raised false deck, then the cabling can enter from the bottom. Otherwise the cable should enter the rack from the lower half of the rear panel. For all cable entrances, a minimum of three inches of slack should be provided to allow for movement of the rack under shock and vibration. There should also be a minimum length of 18 inches between the last cable support and the cable's entrance to the equipment.

Racks should be ordered with removable, but lockable, side, front and rear panels for maximum equipment accessibility. Note that the location of louvers in rack panels depends upon the cooling method that is used (see below).

The location of equipment within racks is a trade-off among the sometimes conflicting parameters of accessibility, weight, and cooling. Heavy equipment should be located low in the rack for stability and ease of removing. Equipment that requires reading of displays, LEDs, or patching should be located at eye level. Heat-dissipation equipment should be located near the air exhaust, not near the cold air inlet, to avoid pre-heating the air flowing over the rest of the equipment.

Heavy equipment should be mounted using front-to-rear angle brackets or slide trays to simplify installation and removal, and to avoid the need to carry the weight of the equipment on the front-panel screws.

4.4.1.1 Cooling

Racks that contain equipment whose total power dissipation is more than 100 watts should be provided with rack-mounted blowers or fans to augment any cooling that might be provided by fans inside the equipment.

The cubic-feet-per-minute (CFM) rating of the rack blower/fans can be estimated from the following equation:

$$CFM = 4P/T$$

where

CFM = airflow in cubic feet per minute

P = Total rack power dissipation in watts

T = Temperature rise (inlet to outlet) in degrees Fahrenheit.

For example, a rack with 1000 watts of electronics will need a 400-CFM blower to limit the temperature rise to 10 ^{o}F.

Since heated air tends to rise, the airflow from fans or blowers should be bottom-to-top. This means placing a blower at the bottom of the rack, or an exhaust fan at the top of the rack. In either case, a washable air filter should be placed at the air entry point. Note that the blower, as opposed

to the exhaust fan, has the added advantage of putting a positive pressure within the rack to keep out dust and dirt from unfiltered air entry.

If a blower is placed at the bottom of the rack, then the rear and/or side panels should have louvers near the top for exhaust air to exit. Do not use fully-louvered panels that would short-circuit the air flow. If exhaust fans are used, then the doors and panels should have no louvers; the cold air enters from the air filter near the bottom and the warm air exits via the top-mounted exhaust fan.

4.4.1.2 Shock Isolation

Shipboard racks should not be hard-mounted to deck foundations, but should be shock isolated via coil springs or other acceptable isolation mechanisms. Tall racks (over 5’ tall) should also have shock-isolated anti-sway mounting from the top of the rack to the bulkhead or to the overhead.

4.4.1.3 Line Conditioning and UPS

Shipboard AC power is notoriously unreliable, noisy, and subject to over-voltage and under-voltage conditions that can seriously damage COTS networking equipment. COTS network equipment should never be connected directly to shipboard power without the protection of a line conditioner and an uninterruptable power supply (UPS). (Printers need not be connected to UPS.)

Line conditioners protect against over/under voltage conditions, and provide some degree of noise suppression, but do not protect against total loss of power. UPSs provide over/under voltage protection, noise suppression, and supply AC power (generated from DC batteries within the UPS) for a limited time. (The loss-of-power protection interval varies with the size of the UPS batteries, but is typically about 15-20 minutes when the UPS is operated at 50% of rated load.)

Unlike shore-based AC distribution systems, shipboard power uses an ungrounded (floating) neutral. If ordinary line conditioners or UPSs are connected to shipboard power, the grounded neutral will cause a ground-fault indication. Line conditioners and UPSs with floating neutral can be obtained, but they must be special-ordered for shipboard service.

4.4.2 Electrical System Interfaces

4.4.2.1 Electric load analysis

Prior to installation, an electric load analysis should be performed to calculate the electrical system impact associated with the new equipment, taking into consideration any removed equipment as well.

4.4.2.2 Local distribution

If adequate electrical distribution is not available to supply the new loads, install additional equipment and cable as required. All electrical installations should be in accordance with DOD-STD-2003. All electrical cabling should be in accordance with MIL-HDBK-299. If the existing electrical distribution system is modified, circuit breakers and cables should be examined for adequacy and modified or replaced as necessary to support the new loads.

4.4.2.3 Bonding and grounding

Secure electrical information processing equipment and cables should be bonded and grounded in accordance with MIL-STD-1680. All other equipment and cable shields should be bonded and grounded in accordance with MIL-STD-1310. Bonding straps required should be fabricated in accordance with MIL-S-24729.

4.4.2.4 Power Source for Backbone Switches

Backbone switches should be supplied AC power from two independent power sources via an automatic power bus transfer system.

4.4.3 Air Conditioning

Prior to installation, the ability of the existing ship's air conditioning system (High Volume Air Conditioning (HVAC) system) to support the equipment installations in each compartment on the ship must be verified. If required, the air conditioning system should be modified in accordance with NAVSEA 0938-LP-018-0010.

4.4.4 Satellite Communication Equipment Requirements

Both military and civilian Satellite Communication (SATCOM) Systems installation requirements are coordinated between the originating Program Office and the Naval Sea Systems Command (NAVSEA). Positioning of above deck equipment such as antennas and remote amplifiers is controlled by mission requirements, suitable installation facility sites, and programmatic realities. Issues typically addressed include:

- Safe access by maintenance personnel
- One-antenna installation
    - Unobstructed visibility of the sky
- Two-antenna installation
    - Maximize the look angles of mutual coverage and provide total visibility of the sky
- Stable antenna mounting surface that does not oscillate during antenna motion
- Close proximity to below-deck equipment to reduce control and signal line losses
- Analysis of ships overturning moments

Figure 4-3 provides weight, volume and power characteristics for each shipboard SATCOM system.

Equipment Name	Above Deck Equipment		Below Deck Equipment		Power (W)
	Deck Surface Area (m^2)	Weight (kg)	Volume (m^3)	Weight (kg)	
UHF SATCOM					
AN/WSC-3	5	240x2	0.1	148	600
AN/SSR-1	1	20	0.1	20	200
SHF SATCOM					
AN/WSC-6	5	272	5	500	50,000
AN/SSC-6	3	272	43 (van)	1500 (van)	69,000
AN/WSC-2	6	1,225	7	900	32,000
AN/SSC-7	3	500	5	550	16,000
EHF SATCOM					
AN/USC-38 SHIP	5	550	1.2	737	4275
AN/USC-38 SUB	0.05	40	1.1	692	4050
Commercial SATCOM (INMARSAT & other high data rate systems)					
Inmarsat-A	1.2	100	0.05	20	300
Inmarsat-B	1.2	100	0.05	20	300
Inmarsat-C	0.02	2	0.05	3	150
Inmarsat-M	0.3	30	0.05	20	200
Intelsat, DirectPC, Orion, Teledesic, Celestri	Certified shipboard data is not available				

Figure 4-3. SATCOM Nominal Physical Characteristics

4.4.5 Special Considerations for Shipboard Mission Critical Signals

4.4.5.1 Shock

Equipment shall meet grade A shock requirements. Equipment shall operate before, during and after shock conditions resulting from high impact shock testing of hardware, mounting rack, and shock mounting devices. For critical signals that cannot accept momentary disruption of a circuit, multi-mode fiber is preferred over single-mode fiber because multi-mode fiber connectors withstand shock more readily than single-mode connectors.

4.4.5.2 Humidity

Using COTS hardware in environments with condensing 100% relative humidity can lead to shorting of printed circuit cards which are normally not conformally coated in COTS equipment. One solution to this problem is the use of specially treated equipment rooms (node rooms) or controlled spaces where highly-reliable air conditioning is always available.

4.4.5.3 Temperature

Most COTS electronic equipment is designed to temperature ranges of 0°C to 30°C, 40°C or 50°C. Shipboard operation outside of this range can cause failure or improper operation of LED displays, hard drives and CD-ROM drives at the low temperature extremes, and power supplies and other electronics at the higher temperature extremes. The concept noted in the previous paragraph of air-conditioned node rooms can be used to solve this problem. Temperature testing shall be tailored in accordance with MIL-STD-810, Method 501 or Method 502 and conducted with the equipment operational in a controlled environment of 0° C to 50°C.

4.4.5.4 Magnetic Field

The high magnetic fields caused by ship degaussing can disturb the displays on CRT screens. If critical information needs to be read during degaussing, consider the use of flat-panel displays instead of CRT displays.

4.4.5.5 Vibration

Each rack of COTS equipment and workstations, including shock mounts if used, must be tested for vibration response per the tailored requirements of MIL-STD-167/1. Equipment shall be subjected to endurance testing at fixed frequencies based upon the critical frequencies determined from the vibration response testing. When vibration response investigation does not identify any critical frequencies, testing shall be conducted at the maximum vibration frequency of 50 Hz and .076 mm vibration amplitude.

4.4.5.6 Electromagnetic susceptibility

Electromagnetic susceptibility requirements shall be tailored in accordance with MIL-STD-461. The equipment shall not be susceptible to electromagnetic emission in the room or area in which it is installed.

4.4.5.7 Electromagnetic emissions

Electromagnetic emissions requirements shall be tailored in accordance with MIL-STD-461. Electromagnetic emissions tests shall be tailored in accordance with MIL-STD-462. COTS equipment may be procured to FCC Class A or B regulations in accordance with 47 CFR15, and modified to conform to the requirements of the shipboard installation, through application of EMI filters and shielding

4.4.5.8 Fungus/mold

The equipment shall not support fungal or mold growth. Fungus/mold tests shall be tailored in accordance with MIL-STD-810.

4.4.5.9 Salt Fog

Equipment shall be tested to withstand salt fog when used in shipboard locations that are susceptible to salt fog conditions. Salt fog tests shall be tailored in accordance with MIL-STD-810.

4.5 Shore-based Facility Requirements

Shore-based Naval installations are located in virtually every geographic area, with a broad range of mission requirements and environmental conditions. Consequently, facility engineers consider each information technology facility's unique requirements, and custom engineer facilities to satisfy requirements within the constraints of security, construction standards, equipment requirements and available space.

4.5.1 Architectural Components:

Architectural component standards comprise the building blocks that the information technology building or facility is built around. Where IEEE, ITU, MIL SPEC, or other standards apply, they are listed after the component description.

- Walls – drywall, masonry, plaster.
- Ceiling – drywall, suspended, plenum.
- Flooring – generally raised floor system (must be grounded).
- Finishes:
  - Carpet – must be static controlled.
  - Vinyl floor tile must be conductive floor finish.
- Additionally, the following generic points apply to all information technology facilities.
- All ceiling, wall and floor penetrations must be sealed.
- Door Hardware – security requirements may call for specialized entry systems.
- Sufficient space to easily move around the equipment.

4.5.2 Fire Protection Components:

Information technology computing and data storage equipment represents a significant investment that must be protected from catastrophic failure due to fire. Due to factors that are designed to protect human life and data integrity, traditional fire-fighting measures such as Halon extinguishers or water are unacceptable. Additionally, power-kill-switches are highly recommended. Standards for fire protection components are:

- CO_2
- Emergency Power cut off may be required for some systems

4.5.3 Mechanical Components:

Mechanical components incorporate environmental controls, and physical housing for equipment. Associated standards are:

- Critical humidity control in accordance with equipment manufacturer's recommendations
- High Volume Air Conditioning or individual room units control in accordance with equipment manufacturer's recommendations
- Special equipment noise restrictions.

4.5.4 Electrical Components

Power requirements for commercial and military information technology equipment vary widely dependent on geographic location (US 115VAC, EUR 220VAC), direct current versus alternating current, and requirements for availability under adverse circumstances. The guidance below lists factors that must be considered for supplying this critical component.

- Power systems – may require red/black power for security
- May require separate 20 amp service for the network equipment and servers
- Uninterrupted Power Supply (UPS) dependent upon service or data criticality
- Individual panel boards with shunt trip circuit breakers
- Specialized cabling requirements
- Specialized lighting requirements
  - Direct or indirect
  - Type of lighting fixtures
- In order to ensure that your specific requirements are satisfied the following references for electrical systems address military and commercial standards:
  - MIL-HDBK-1004/1 Preliminary Design Considerations.
  - MIL-HDBK-1004/2A Power Distribution Systems.
  - MIL-HDBK-1004/3 Switch gear and Relaying.
  - MIL-HDBK-1004/4 Electrical Utilization Systems.
  - MIL-HDBK-1004/5 400 Hz Mcd-Volt. Conversion/Distribution & Low Voltage Systems.
  - MIL-HDBK-1004/6 Lightning and Cathodic Protection.
  - MIL-HDBK-1004/7 Wire Communications & Signal Systems.
  - MIL-HDBK-1008C Fire Protection for Facilities Engineering.
  - MIL-HDBK-1012/1 Electronics Facilities Engineering.
  - MIL-HDBK-1012/3 Telecommunications Premises Distribution Plan, Design.
  - DM 13.02 Commercial IDS.
  - ANSI C2 1997 National Electrical Safety Code.
  - NFPA 70 1996 National Electrical Code.
  - NFPA 72 1993 National Fire Alarm Code.
  - NFPA 780 1995 Lightning Protection Code.

4.6 Ground Combat Environment

Computers and communication equipment to be used in ground combat operations should be ruggedized and portable. This section will be completed in future versions of the ITSG.

4.7 Naval Aircraft Environment

Commercial off-the-shelf (COTS) equipment can reliably operate within enclosed air-conditioned spaces of aircraft facilities provided that some reasonable and practical installation guidelines are followed. Aircraft have very unique requirements that should be addressed by the program manager (PMA) for the applicable platform. Even different versions of the same aircraft platform may have specific requirements that differ significantly from previous versions.

At a minimum, the following areas should be addressed when considering application of COTS information technology solutions onboard DON aircraft:

- Racks
- Cooling
- Shock Isolation
- Vibration
- C/G effects
- Line Conditioning and UPS
- Electrical system interfaces
- HVAC system interfaces
- Satellite antenna interfaces
- A/C data bus interfaces

4.8 References

4.8.1 Standards and Specifications Resources

4.8.1.1 Security

Secretary of the Navy (SECNAV), “Department of the Navy Information Security (INFOSEC) Program” SECNAVINST 5239.3; 14 July 1995; http://www.cnet.navy.mil/tralant/scnv5239.pdf (23 May 1997)

Department of Defense (DoD); “National Industrial Security Program Operating Manual (NISPOM)”, January 1995; http://www.fas.org/sgp/library/nispom.htm (23 May 1998)

Department of Defense (DOD) MIL-STD-461D “Electromagnetic Interference Emissions and Susceptibility, Requirements for,” 11 January 1993, www.library.itsi.disa.mil/org/mil_stdb/ms461d.html (23 May 1998)

National Security Agency (NSA); “National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST 2/95, RED/BLACK Installation Guidance”; 12 December 1995

4.8.1.2 Shipboard Cable Plant

Naval Sea Systems Command (NAVSEA) “NIIN IPT Near-Term Guidance for Shipboard Networks”; 11 November 1997

Naval Sea Systems Command (NAVSEA) “Shipboard Cable Plant Management System Functional Specification” 29 November 1996

Department of Defense (DOD) MIL-STD-167/1 “Mechanical Vibrations of Shipboard Equipment (Type I & II)” 1 September 1993, http://diamond.spawar.navy.mil/specs/mil_std/MIL_STD_167.html (23 May 1998)

Department of Defense (DOD) MIL-STD-461D “Electromagnetic Interference Emissions and Susceptibility, Requirements for,” 11 January 1993 Web: library.itsi.disa.mil/org/mil_stdb/ms461d.html (23 May 1998)

Department of Defense (DOD) MIL-STD-462 “Electromagnetic Interference Characteristics, Measurement of” 11 January 1993, www-library.itsa.disa.mil/org/mil_stdb/ms462d.html

Department of Defense (DOD) MIL-STD-810E “Environmental Test Methods and Engineering Guidelines” 1 September 1993, www-library.itsa.disa.mil/org/mil_stdb/ms810e.html

MIL-STD-2042

MIL-HDBK-2051

DOD-STD-1678

MIL-T-29504/14 &/15

MIL-F-49291

MIL-C-85045

MIL-I-24728

MIL-C-28876

MIL-S-24623

MIL-C-83522/16

4.8.1.3 Shore Base Cable Plant

American National Standards Institute (ANSI)/Telecommunications Industry Association (TIA)/Electronics Industries Alliance; Standard 568A: Commercial Building Telecommunications Cabling Standard, October 1995, http://www.cis.ohio-state.edu/hypertext/faq/usenet/LANs/cabling-faq/faq-doc-9.html (23 May 1998) and http://diamond.spawar.navy.mil/cabling/C_2_1.html (23 May 1998)

American National Standards Institute (ANSI)/Telecommunications Industry Association (TIA)/Electronics Industries Alliance; Standard 569: Commercial Building Standards for Telecommunications Pathways and Spaces; October 1990; http://diamond.spawar.navy.mil/cabling/C_2_5.html (23 May 1998)

4.8.1.4 Shipboard Electrical System

DOD-STD-2003

MIL-HDBK-299

MIL-STD-1680

MIL-STD-1310

MIL-S-24729

4.8.1.5 Shipboard Air Conditioning

Naval Sea Systems Command; NAVSEA 0938-LP-018-0010: Shipboard Air Conditioning.

4.8.1.6 Shore Electrical System

Department of Defense (DOD) MIL-HDBK-1004/1 Preliminary Design Considerations;

Department of Defense (DOD) MIL-HDBK-1004/2A Power Distribution Systems;

Department of Defense (DOD) MIL-HDBK-1004/3 Switch gear and Relaying;

Department of Defense (DOD) MIL-HDBK-1004/4 Electrical Utilization Systems;

Department of Defense (DOD) MIL-HDBK-1004/5 400 Hz Mcd-Volt. Conversion/Distribution & Low Voltage Systems;

Department of Defense (DOD) MIL-HDBK-1004/6 Lightning and Cathodic Protection;

Department of Defense (DOD) MIL-HDBK-1004/7 Wire Communications & Signal Systems;

Department of Defense (DOD) MIL-HDBK-1008C Fire Protection for Facilities Engineering;

Department of Defense (DOD) MIL-HDBK-1012/1 Electronics Facilities Engineering.

Department of Defense (DOD) MIL-HDBK-1012/3 Telecommunications Premises Distribution Plan, Design.

DM 13.02 Commercial IDS

American National Standards Institute (ANSI); ANSI C2-1997: “National Electrical Safety Code”; 1967; www.nssn.org (23 May 1998)NFPA 70 1996 National Electrical Code.

National Fire Protection Association (NFPA); Document 70: “National Electrical Code” 1996, www.nfpa.org (23 May 1998)

National Fire Protection Association (NFPA); Document 72: “ National Fire Alarm Code” 1993, www.nfpa.org (23 May 1998)

National Fire Protection Association (NFPA); Document 780: “Lightning Protection Code” 1995, www.nfpa.org/ (23 May 1998)

4.8.1.7 Shipboard SATCOM Equipment

Navy UHF Satellite Communications System Description, FSCS-200-83 of 1 August 1984

Navy SHF Satellite Communications System Description, NSHFC 301 of November 1983

AN/WSC-6(V) Navy 8kW SHF SATCOM literature from Raytheon Company.

AN/USC-38(V) Navy EHF SATCOM Terminal literature from Raytheon Company

4.8.2 Supporting Resources

Additional information can be found at the Web sites listed below.

Heavy-Duty Equipment Racks for Shipboard Use

Equipto Electronics Corporation web site; www.equiptoelec.com (23 May 1998)

Shock Mounts for Shipboard Racks

Aeroflex International Inc web site; www.aeroflex.com (23 May 1998)

UPS and Power Conditioners for Shipboard Use

American Power Conversion (APC) web site; www.apcc.com (23 May 1998) (Their X93 series has been specially modified to meet floating neutral wiring shipboard wiring requirements.)

Clary Corporation web site; www.clary.com (23 May 1998)

5. Information Transfer

This chapter includes network communication standards and guidance for terrestrial wide area networks, wired and wireless local area networks, satellite communication networks, and internetworking protocols to link these together into a single integrated network. The relationship of this chapter with the ITSG is shown in Figure 5-1.

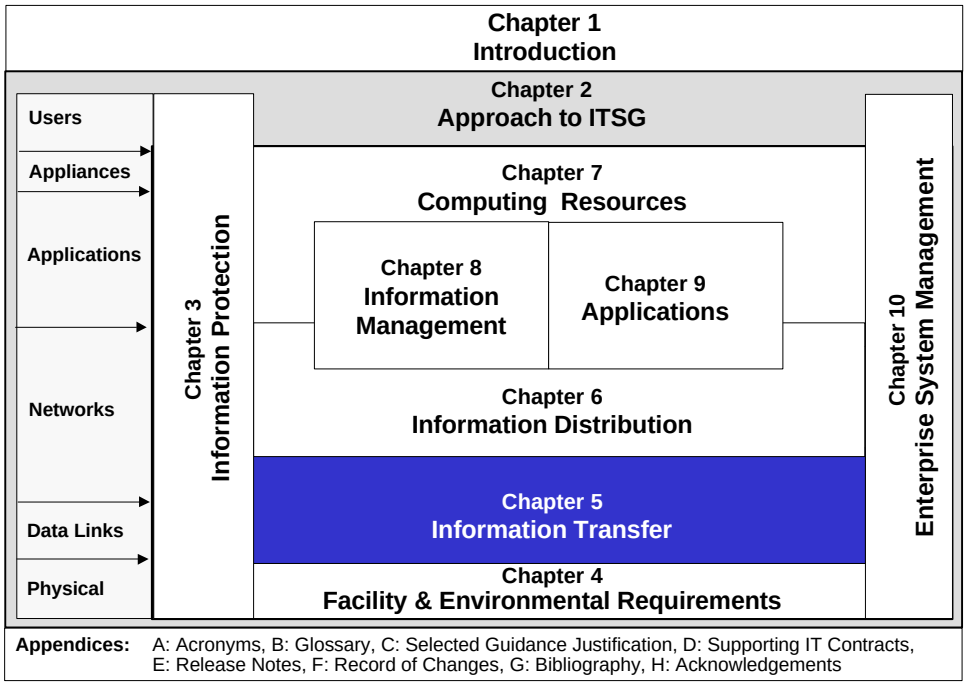


Figure 5-1. ITSG Document Map Highlighting Chapter 5, Information Transfer

5.1 Overview

Information Transfer encompasses the first four layers of the seven-layer International Standards Organization/Open Systems Interconnect (ISO/OSI) model: physical, data link, network and transport.[3] The proper selection of interface standards and protocols specified in this chapter will promote an interoperable and scaleable communications infrastructure for DON systems installed in each operational environment.[4]

The Navy and Marine Corps rely on voice, data, facsimile, video, and imagery at ever-increasing rates. The underlying infrastructure must be capable of supporting multimedia, offer a variety of quality-of-service options (to meet application bandwidth, delay and priority constraints), be scaleable in both size complexity and available bandwidth, and assure interoperability among other DOD and commercial information systems. The need for the user to interact with information and systems outside of their immediate surroundings is expanding – architectures must be global for

[3] In the Internet Protocol (IP) model, the Network and Transport layers are combined. Also, detailed descriptions of the physical cable plant are provided in Chapter 4.

[4] Operational environments are described in Section 2.6

our geographically dispersed and mobile commands but retain a local “look and feel” for operation.

Our information services can best be provided by a network-centric approach in which services and applications are built onto a robust, scaleable and survivable network infrastructure. This network infrastructure must provide an adaptable foundation for advances such as multicast (in which information is broadcast to either a small or wide range of users in an efficient manner), real-time systems (which have strict time-sensitive and priority requirements) and other fleet priority systems.

5.1.1 Operational Environment Considerations

The standards described here are for the most part generic to any DON environment. However, platform-specific issues are addressed where appropriate.

5.1.1.1 Shipboard

Shipboard networks, including those on submarines, require special consideration. Their operational requirements are extraordinarily demanding, their off-board bandwidth environment is constrained, and their facility and support requirements are unique. To satisfactorily address these challenges, commanders must base their implementations upon the specific guidance for networks aboard new construction and in-service ships in this document. These standards must address all mission critical systems requirements and include both hardware and software functions as part of the initial design and installation of a shipboard network. In addition, interfaces between real-time systems (e.g., fire control, weapons control systems) and non-real-time systems must strive to achieve interoperability.

5.1.1.2 Shore

Shore-based networks, especially those in R&D activities and system command centers, offer additional flexibility to take greater risks and to drive the design of deployable systems. These environments are needed to push the emerging technologies.

5.1.1.3 Ground

Current standards for deployed ground forces consist mainly of point-to-point Radio Frequency (RF) links. This will change as RF-based networks are developed. Until such time, however, networking guidance for ground forces is limited to that provided for small installations.

5.1.1.4 Aircraft

Aircraft represent a unique environment in that their internal networks are small. The information transfer standards, however, remain the same. As with deployed ground forces, future RF-based networks will be important in fulfilling the aircraft mission.

5.1.1.5 Spacecraft

The satellite environment is undergoing a major change. Historically, satellite links are described as “bent pipes” in which information is uplinked to a particular spacecraft and simply repeated or retransmitted downward. Systems currently being designed will behave as true networks in which the original data will be routed along a dynamically changing subset of satellites in the

"constellation" before being relayed back to earth. Access to these satellite networks will be through proprietary ground terminals via standard interfaces.

5.1.1.6 Individual Mobile Users

Transportable and mobile users are considered in this document although applicable standards are still evolving. A distinction is made between users who transport their nodes from one place to another without maintaining connectivity and those who *do* maintain connectivity. In either case, it is desirous to have users "take their environment with them".

5.1.2 Adopted Network Definition

The "area network" conventions adopted by the ITSG are shown in Figure 5-2.

Local Area Network (LAN). LAN*s* use the IEEE 802, ANSI, and ATM standards – the signals travel over optical fiber cable or copper wire and all network components are under the ownership and control of the network manager. They include wireless LANs that are generally designed to support untethered network-to-end-user connections. The control definition applies here. Extended LANs include base and campus networks

Wide Area Network (WAN). WANs are divided into two parts. The first is defined as trunk technology and switching (Telephony DS-n/T-n and Synchronous Optical Network (SONET) OC-n transport, and ATM and Frame Relay switching). For this part, the economic definition applies – the LAN provider will generally purchase these services rather than invest in wide-area equipment and cable. The second addresses what the telephone industry refers to as the "local loop", meaning the reach from the central office to the business or residence. In many cases, the customer may actually own such assets. (See Table 5-1 for an illustration of DS, T and OC link designations).

Metropolitan Area Network (MAN). MANs cover that ambiguous overlap where relatively wide area networks can take on the characteristics of a LAN or a WAN. MANs either use LAN technology extended over a "larger" regional area or use WAN technology – point-to-point links that connect a relatively high concentration of LANs together, within a "smaller" regional area.

Radio Communications to Dispersed Forces include Satellite Communications (SATCOM) and Line-of-Site (LOS) radio links to support trunk (router-to-router or switch-to-switch) connections to underway or deployed forces.

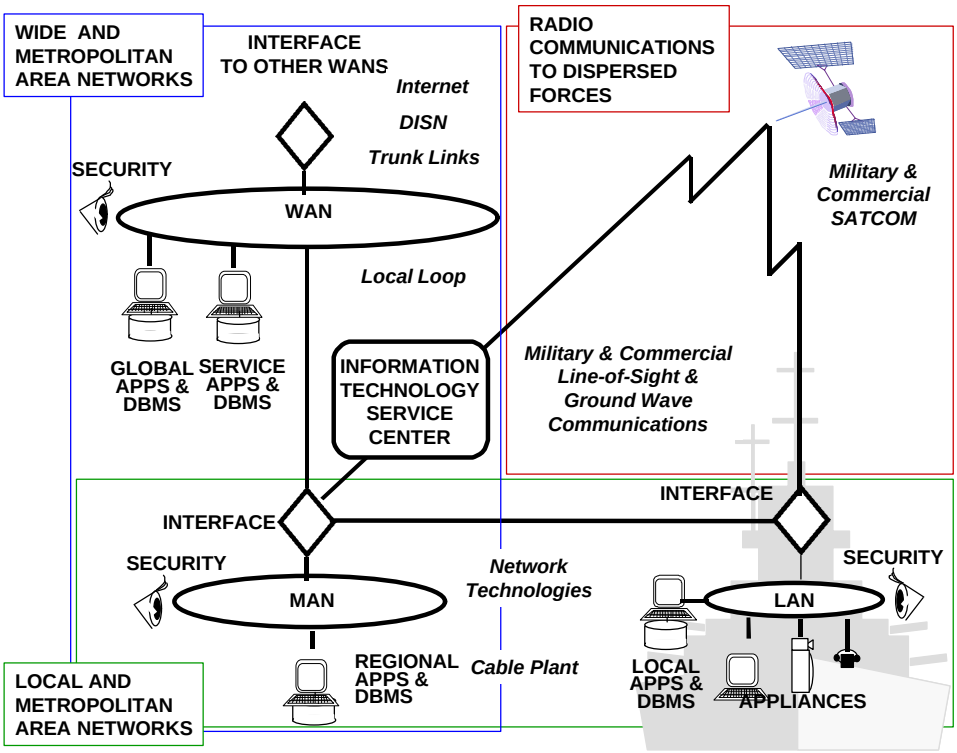


Figure 5-2. Adopted Architecture Model for LANs, MANs, WANs, and Radio Communication to Dispersed Forces

5.1.3 Performance Issues

To successfully design the information transfer infrastructure, system architects must ensure that operational requirements, including those of mission critical systems, are satisfied by the performance characteristics of the supporting IT systems. This is a challenging task, but new technologies are continually emerging that, if implemented in a standards compliant architecture, can dramatically improve the robustness of our infrastructure.

Throughput. Data throughput capacity is an important consideration in designing LANs and WANs. In the past, networks covering campuses and other small geographic distances could support significantly larger transfer rates than those that spanned large distances. Figure 5-3 illustrates the evolution of throughput over the last 20 years and Table 5-1 provides commonly used data rate designations. For example, in 1980 LANs employed 10 Mbps Ethernet while WANs employed 64 Kbps, DS-0 or 1.5 Mbps DS–1 for regional and long haul channels. This rate disparity began to diminish as LAN transfer rates increased to 100 Mbps through Fiber Distributed Data Interface (FDDI) and Fast Ethernet while WANs employed 45 Mbps, DS-3. Presently, transfer rates for local and long-haul networks have reached parity with OC-3/OC-12 SONET/ATM equipment and service. Future products are expected to continue this trend with 2.4 Gbps (OC-48) and 9.6 Gbps (OC-192) systems as well as Wave Division Multiplexing (WDM) technology (supporting 10’s and 100’s of independent 9.6 Gbps streams). As WAN transfer rates become comparable to those of the LANs, design emphasis must be placed on minimizing excessive processing of Protocol Data Units (PDUs) as they cross WAN-LAN boundaries (routers, firewalls, network filters, etc.).

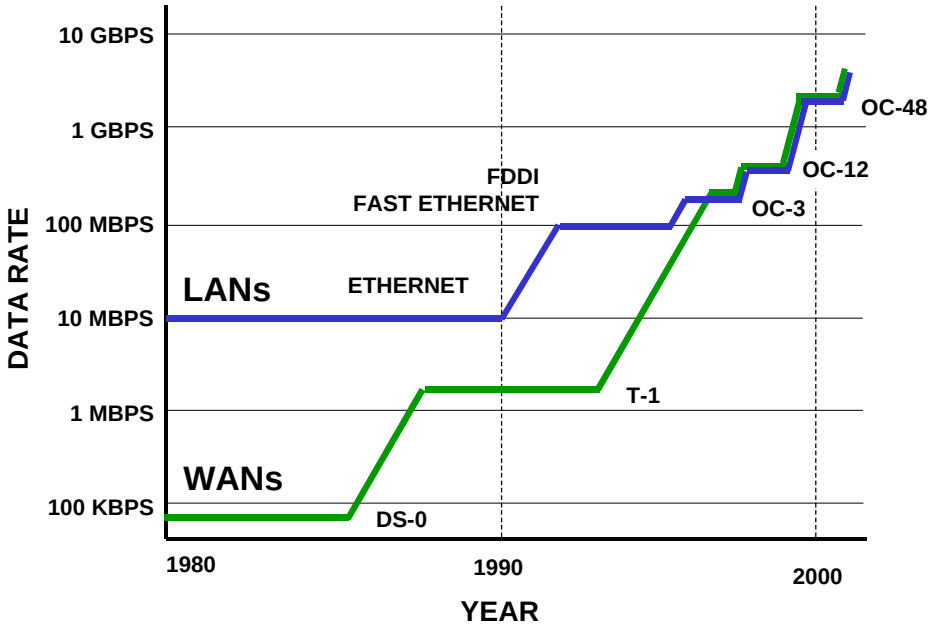


Figure 5-3. Evolution of LAN and WAN Data Throughput

Delay. Delay is another significant performance parameter that drives system design. Delay (with respect to networks) is composed of three significant components: propagation delay, processing delay and delay variation (or jitter). Electromagnetic propagation (including physical cables) has physical limitations that cannot be overcome. Propagation delays are simply a function of the geographic distance between points and cannot be reduced beyond these physical limits. By contrast, processing delays are nearly independent of distance and can range from insignificant, for electronic switching, to very significant, for the processing of data packets through CPUs, routers, firewalls, and network filters. Delay variation comes from many sources such as queues, physically different paths, RF media perturbation, etc. Delay variation, with respect to time, is a third design parameter.

Latency. The existing internet protocols provide best-effort service. In addition to the low-latency requirements of real-time systems, a number of applications require deterministic, or bounded-delay, service. Several next-generation initiatives, such as Asynchronous Transfer Mode (ATM), Reservation Protocol (RSVP), and next generation transport protocols, offer the promise of supporting bounded delay applications over a multi-segment internetwork. The recommended standards in this chapter will position the infrastructure to accommodate this capability as it matures.

Other performance measures may be used when the system has more rigid design constraints. For example, when designing for survivability in shipboard environments, the following apply:

Network Availability. The following network equipment performance requirements are necessary to support mission critical systems. The following operating modes are defined: normal, failure, and casualty. Normal mode is defined to be all network devices available and functioning. Failure mode is defined to be the malfunctioning of any two randomly selected network devices. Casualty mode is defined to be the non-availability of 25 percent of populated network port capacity. The network circuit availability of any single-homed user-to-user circuit shall be 0.999 or greater. The network availability of any redundant dual-

homed user-to-user circuit shall be 0.9999 or greater. The network system availability for mission-critical applications shall be 0.9999 or greater.

Data Rate Designation	Data Rate (rounded down)	Voice Quality Circuits 64 kbps	Full Motion Video Circuits 1.544 Mbps (note 1)	Remarks
DS0	64.0 kbps	1	-	Data Service - 0
T1	1.5 Mbps	24	1	Transmission Carrier -1
DS1	1.5 Mbps	24	1	Data Service - 1
DS1C	3.1 Mbps	48	2	Data Service - 1C
DS2	6.3 Mbps	96	4	Data Service - 2
Ethernet	10.0 Mbps	156	6	CSMA/CD (Note 2)
T3	44.7 Mbps	672	28	Transmission Carrier -3
DS3	44.7 Mbps	672	28	Data Service - 3
OC-1	51.8 Mbps	810	33	Optical Carrier - 1
Fast Ethernet	100.0 Mbps	1562	60	CSMA/CD (Note 2)
DS4N4	139.2 Mbps	2016	84	Data Service – 4N4
OC-3	155.5 Mbps	2430	101	Optical Carrier - 3
OC-9	466.0 Mbps	7218	301	Optical Carrier - 9
OC-12	622.0 Mbps	9720	405	Optical Carrier - 12
OC-18	933.0 Mbps	14,578	604	Optical Carrier - 18
Gigabit Ethernet	1.0 Gbps	15,625	647	CSMA/CD (Note 2)
OC-24	1.2 Gbps	18,750	777	Optical Carrier - 24
OC-36	1.9 Gbps	29,678	1230	Optical Carrier - 36
OC-48	2.5 Gbps	38,875	1619	Optical Carrier - 48
OC-96	4.9 Gbps	77,750	3239	Optical Carrier - 96
OC-192	9.6 Gbps	150,000	6217	Optical Carrier - 192

Table 5-1. Data Rate Designations

Note 1: Maximum value required for 30 frames/sec. Achievable at data rates as low as 384 kbps through compression.
Note 2: Carrier Sense Media Access / Collision Detect.

5.2 Physical and Data Link Layers

The physical and data link layers describe the lowest level of the ISO/OSI model (Figure 5-4). The physical layer is the actual channel on which data is transferred. The data link layer describes the protocol used directly on the physical layer medium. While the ISO/OSI describes these layers as separable, in practice they are tightly linked. In fact, there is usually a small number of recommended data link layer protocols associated with a particular physical layer specification and vice versa. Therefore, these bottom two layers will be discussed together.

Physical channels include the fiber, copper and radio media upon which the data signals travel. Standards and. guidance associated with the cable plant are covered in Chapter 4. Radio media is discussed in Section 5.2.3.

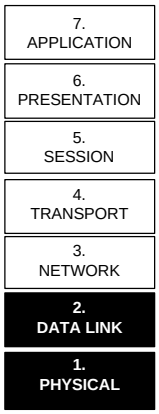


Figure 5-4. ISO/OSI model layers 1 and 2.

5.2.1 Local and Metropolitan Area Network Physical and Data Link Layer Technologies

Best Practices

The preferred network architecture is a mesh topology of optical fiber running SONET on the physical layer and ATM on higher layers. Drop links to servers should be SONET/ATM linked to two physically separated switches. Appliances (end user devices) should be linked via fiber running (in order of preference) ATM, Switched Fast Ethernet, or Switched Ethernet. Category 5 UTP copper cable is permissible for the drop cable to non-mission critical appliances.

LAN configurations for the backbone, servers, mission critical appliances, and non-mission critical appliances should be consistent throughout the information system domain. Mixing of different protocols on like architectural components (e.g., all non-critical appliances) is not permitted except temporarily during the migration to an advanced protocol.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
ARCnet 100VG AnyLAN (802.12) Token Ring FDDI/UTP ANSI X3T12 SNA/APPN Novell IPX NetBEUI OpenAir 2.4 Wireless ETS 300 653 HIPERLAN Wireless	Switched Ethernet Switched Fast Ethernet FDDI SONET ATM UNI 3.1 for ATM PNNI Phase 1 for ATM	Switched Ethernet Switched Fast Ethernet SONET ATM UNI 3.1 for ATM UNI 4.0 for ATM PNNI Phase 1 for ATM	Switched Fast Ethernet SONET ATM UNI 3.1 for ATM PNNI Phase 1 for ATM UNI 4.0 for ATM	SONET ATM UNI 4.0 for ATM PNNI Phase 1 for ATM	Gigabit Ethernet IEEE Std 802.11-1997 (FHSS, 2 Mbps, 4-level GFSK) Wireless PNNI Phase 2 for ATM WDM
Activities, Platforms, Operational Environments		All			

Table 5-2. Physical and Data Link Recommended Implementations for LANs

There are a large number of technologies that fit in the physical and data link layer that can potentially be used in naval facilities. In the interest of balancing application flexibility with the logistics advantages of standardization, ITSG limits the selection to one, or a combination, of the following four network technologies: Ethernet, Fast Ethernet, FDDI and ATM.

Advantages and disadvantages of these lower layer networking technologies vary with the specific application, and are summarized in Figure 5-5.

Technology	Advantages	Disadvantages
Ethernet (10 Mbps)	Well understood Inexpensive Numerous vendors Strong commercial support Reliable multi-vendor interoperability Available in fiber version	Low throughput High latency Not scaleable as a backbone No fault tolerance No Quality of Service
Fast Ethernet (100 Mbps)	Moderate throughput Numerous vendors Strong commercial support Reliable multi-vendor interoperability Available in fiber version	Not scaleable as a backbone No fault tolerance No Quality of Service
FDDI (100 Mbps)	Moderate throughput Deterministic latency Fault tolerance Reliable multi-vendor interoperability Relatively easy upgrade from 10 Mbps Ethernet Inherently fiber	Expensive Not scaleable as a backbone without the use of FDDI switches Questionable future COTS support
ATM (155/622 Mbps)	High throughput Non-blocking Scaleable backbone Scaleable host performance Popular in WAN No need for routers to cross LAN/WAN boundary Available in fiber versions • Fault tolerance • Voice, Video and Data integration • Quality of Service	Limited multi-vendor interoperability Incomplete standards Limited multicast and broadcast support

Figure 5-5. Summary of Lower Layer Networking Technology

5.2.1.1 Ethernet

Ethernet is the most well understood networking technology in the commercial and tactical world. Ethernet is widely available in two different data rates: 10 Mbps and 100 Mbps.

Ten Mbps Ethernet is appropriate in situations that do not require extensive bandwidth and where cost is a driving issue. (Most network-ready devices and workstations have embedded 10 Mbps Ethernet.

Ten Mbps Ethernet is used for low-end workstations, but not for the backbone unless it is cost-driven; the implementation has a small number of users and is unlikely to expand.

5.2.1.2 Fast Ethernet

Fast Ethernet (100 Mbps) is the next generation of Ethernet technology and is undergoing wide deployment. Fast Ethernet is viable for the desktop and will soon be available pre-installed on PC motherboards. Note, however, that the fiber version (100BaseFX) is recommended for Navy shipboard use, not the unshielded twisted pair version (100BaseT).

Fast Ethernet may be used for workstation connections, but should not be used for the backbone unless it is cost-driven and the impact of its fixed, non-scaleable bandwidth and lack of inherent fault tolerance are understood, fully evaluated and meet the application requirements.

5.2.1.3 Gigabit Ethernet

Gigabit Ethernet, despite the name, is not based on traditional broadcast Ethernet. It is a point-to-point protocol that is expensive compared to other technologies, e.g. 10 Mbps to 100 Mbps Ethernet or ATM. It is a short-hauled router interconnect technology and not a WAN technology and has limited end station support. Gigabit Ethernet is an emerging technology, and its use is discouraged.

5.2.1.4 Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) is a 100 Mbps networking technology that uses counter-rotating token rings to provide moderate throughput with built-in fault-tolerance. Also, it has bounded deterministic delays, such as how long a station must wait before it can transmit, or how long it will take for a ring to reconfigure after segmentation.

FDDI technology is a technology for use where the advantages of rapid reconfiguration and bounded latency outweigh the uncertainty of future industry support. (The cost of FDDI has not reduced as other networking technologies. With its limited throughput and non-scaleability, vendors are pursuing other high-speed LAN/WAN technologies.) Where FDDI is used, it should be the standard fiber version; the copper version (sometimes called CDDI, FDDI/TP or FDDI/UTP) should not be used.

FDDI may be used for both critical workstation connections and for the backbones of a special purpose networks (e.g., for combat systems). However, FDDI should not be used as a shipwide backbone unless the impact of its fixed, non-scaleable bandwidth is understood and meets the application requirements.

5.2.1.4.1 Standalone Optical Bypass Switches

Optical bypass switches can be used to ensure that an FDDI ring does not segment in case of an end system losing power. However, it is preferable to design FDDI networks in such a way that standalone optical bypass switches are not needed. Optical bypass switches are subject to both signal loss and shock failures.

5.2.1.5 Synchronous Optical Network (SONET)

SONET is the ANSI broadband networking standard designed to meet the needs of high-bandwidth applications, increased data traffic, faster speeds, improved performance and a much greater degree of survivability. SONET uses a closed loop architecture that can recognize a cut or failure, rerouting traffic before serious performance degradation occurs, or in advance of a service interruption. The basic data rates available through SONET are referred to as “Optical Carrier” rates (Table 5-1) and are much higher than available on copper cable. In addition to setting new standard transmission rates, SONET standardizes frame formats and provisioning protocols for Operations, Administration and Maintenance (OAM).

5.2.1.6 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is a networking technology that has several desirable properties such as scalability and quality of service. It is intended to support a large number of users, especially those who require, or will require, multimedia support. It has received wide support in the commercial sector, but associated standards are still maturing.

ATM is a technology that is suitable for the desktop, the backbone and the WAN. The preferred desktop ATM interface is 155 Mbps OC-3c (fiber). The 25Mbps Desktop ATM and the 155-UTP, both of which use unshielded twisted pair, are alternate choices, should cost be an issue. In shipboard environments, however, the use of copper is discouraged so 25Mbps and 155-UTP should be limited.

The 622 Mbps OC-12c interface may be used for inter-switch backbone trunks and high-speed host connections for devices such as servers. Given the use of Private Network to Network Interface (PNNI), the option of using a greater number of less-expensive OC-3c inter-switch trunks as an alternative to a smaller number of OC-12c trunks should be considered as a possible means of increasing the network’s reliability and survivability. (This only applies if the data rates of individual ATM virtual circuits are significantly less than OC-3c.)

ATM is a preferred backbone technology for new construction and major upgrades to all networks. Due to the current state of ATM interoperability, care should be taken when using ATM to assure that the same version of PNNI is used for all switches, and the same version of User to Network Interface (UNI) is used for all switches and workstations.

ATM is making great strides in WAN applications. In addition, many service providers are offering usage-based billing as an alternative to dedicated service. With this billing option, one could have on-demand access to high-speed transfer rates when the mission demanded. For example, one could contract for 155 Mbps peak service yet pay for 50 Mbps average throughput. When a need arose for higher throughput, one could start using more bandwidth through reconfiguration. (This would be much faster than requesting an upgraded circuit.)

5.2.1.7 Redundancy Techniques and Reconfiguration Time

All networks require some level of redundancy, particularly in the shipboard environment. Redundancy can be implemented under three broad techniques:

(a) **parallel transmission** over multiple paths

(b) **single active path** with one or more fail-over paths

(c) **load sharing** over multiple paths

For shore-based environments, option (c) load sharing, offers a cost-effective way to balance the need to provide redundancy against the need to provide bandwidth. Less critical applications could use the extra bandwidth until it was needed by the critical applications.

Redundancy techniques used for shipboard LANs should be limited to those techniques that are widely supported by industry. Special techniques, such as (a) parallel transmission, may be used in subsystems where the need for a particular form of redundancy, or rapid reconfiguration, can overcome the disadvantages of proprietary solutions. However, proprietary redundancy techniques should never be used in the ship-wide backbone.

Reconfiguration time, depending on the application, can be a critical design constraint. For example, a fire-control system would have a much tighter constraint than an administrative e-mail system. The use of proprietary systems to satisfy reconfiguration time criteria should be minimized.

Option (a), parallel transmission, offers the possibility of the most rapid reconfiguration because each receiving device can arbitrarily select one of multiple simultaneous channels, independent of other receiving devices.

Option (b), single active path, results in switchover or reconfiguration times that can range from 10s of milliseconds (in a small FDDI ring using Station Management (SMT) for reconfiguration) to 10s of seconds (for a large network using IEEE 802.1d Spanning Tree for reconfiguration).

Loadsharing with multiple paths typically achieves switchover in 5 to 15 seconds in a small to medium size ATM network using PNNI.

For a ship-wide ATM backbone, it is important to recognize that the current 5-15 second switchover time, combined with load-sharing over multiple paths, occurs only if the ATM switches are running full Phase 1 (or later) PNNI. Phase 0 PNNI (also known as Interim Interswitch Signaling Protocol or IISP) does not provide inherent redundant path reconfiguration. Multiple paths with IISP must be resolved using spanning tree protocol, with its associated 30 - 90 second reconfiguration time.

ATM switches should use Phase 1 (or later) PNNI. The redundancy architecture should exploit PNNI reconfiguration in lieu of spanning tree reconfiguration. For critical subnets where the PNNI reconfiguration times are excessive, FDDI with SMT reconfiguration is preferred, and parallel transmission over multiple paths is a less desirable option.

Note that, for Ethernet or Fast Ethernet networks, the only widely supported, non-proprietary redundancy mechanism is Spanning Tree.

Caution: Any time a dual-homed device is connected to a network running Spanning Tree, the network will reconfigure to resolve the loop created by the dual-homed attachment. For this reason, it is unwise to use dual-homed laptops or other dual-homed workstations that are moved frequently.

For either single active path or load sharing over multiple paths:

- All backbone switches should be interconnected via multiple trunklines to different switches to avoid any single point of failure;
- All edge devices should be dual-homed to two different backbone switches;
- All servers should be dual-homed to two different network connection points.

5.2.1.8 Network Interface Cards (NICs)

When choosing a lower layer network technology to bring the network to a desktop system, the applications on the desktop system may drive the technology selected. Real-time applications, such as voice and video, require different capabilities of the underlying media than word processors and database applications. For example, 10 Mbps Ethernet may meet the requirements for exchanging e-mail and word processing documents between desktop systems, whereas 155 Mbps ATM may be more suitable for desktop systems supporting a full motion, high definition, video application. Care should be taken, however, in buying “too low.” As traditional low rate applications require more band width, and new applications (as web browsing) emerge, one should plan for future growth by acquiring the fastest host interface that one can afford.

5.2.1.8.1 Ethernet NICs

When procuring a system with Ethernet, a NIC that supports auto-sensing 10/100 Mbps is recommended. Also, a fiber optic NIC can be used to support a future upgrade to FDDI or ATM without the need for re-cabling. However, see Chapter 4, Section 4.3.2.2 regarding the permissive use of Category 5 cable under special circumstances.

5.2.1.8.2 FDDI NICs

A station can be either dual-attached station (DAS) or a singly attached station (SAS) to an FDDI ring. A DAS, while more expensive than a SAS, can be configured for higher survivability.

5.2.1.8.3 ATM NICs

There are two key issues to consider when ATM NICs are used in end systems – the User-Network Interface (UNI) and ATM adaptation protocol support.

5.2.1.8.4 UNI (User-to-Network Interface)

When using ATM NICs, the version of UNI that is supported is critical. The UNI specifies how ATM end systems communicate with other ATM end systems and ATM switches. There is currently one acceptable version of the UNI: version 3.1. The newer version (4.0) has been completed, and supporting COTS products will soon be available.

It is required that all end systems using ATM as the underlying media support UNI version 3.1 or higher.

5.2.1.8.5 ATM Adaptation Protocols

When using ATM NICs, the support for specific ATM adaptation protocols must be determined. Currently, there are four options available in COTS ATM NICs:

- Proprietary Adaptations of IP
- Classical IP Over ATM (RFC 1577),
- LAN Emulation (LANE)

- Multiple Protocol Over ATM (MPOA)
- Native ATM.

Note that while LANE and some proprietary adaptations of IP over ATM support broadcast and multicast, RFC 1577 does not.

Proprietary adaptations of IP, Classical IP and LANE are viewed as near-term solutions that will be replaced by Multi-protocol Over ATM (MPOA). (Most ATM vendors have announced their intention to support MPOA and a number have already started to make Beta versions available to selected customers. Since this is a fast-moving area, users should contact vendors directly regarding delivery schedules.) The idea behind these solutions is to emulate the properties of broadcast media (such as Ethernet and FDDI) on ATM, which is a non-broadcast medium. These solutions do not currently take advantage of the quality-of-service features that are inherent to ATM. There are problems with broadcast and multicast traffic. Each protocol employs a server to emulate broadcast and multicast capabilities. This emulation creates throughput, survivability, and scaleability limitations in the approach. The server is a potential bottleneck for multiple broadcast and multicast traffic streams, and is also a single point of failure.

While use of native ATM corrects some of these problems; it introduces others in interoperability. Most ATM NIC software drivers include an Application Programmers Interface (API) that enables applications to access ATM directly, bypassing the transport and network layer protocols. This enables these applications to use certain quality-of-service functions of ATM. Currently, each vendor of ATM NIC cards has a unique, non-interoperable API, and the use of native ATM may preclude the use of COTS software until such time that APIs are standardized. (As of this writing, Microsoft has announced plans for a standardize WINSOCK driver that supports ATM directly. Also, a number of ATM vendors have announced their intention to support X/Open’s XTI API for UNIX systems.)

Best Practices

ATM NIC cards, which support both RFC 1577 and LANE should be used to promote interoperability now. Since MPOA implementations are beginning to emerge, users are encouraged to start with MPOA if it is available from the selected vendor. If an application requires access to the native ATM services, the API that is part of the NIC can still be used. If the multicast and redundancy capabilities of vendor proprietary adaptations of IP are needed, then that protocol can be used as an interim solution pending the availability of MPOA.

5.2.1.9 Network Configuration

5.2.1.9.1 Switched Versus Shared Hubs

Under many conditions, switching hubs provide a considerable performance improvement over shared-media hubs. Switched hubs will reduce packet collisions and provide greater effective bandwidth than shared-media hubs. In FDDI networks, the use of switched hubs would result in long (Spanning Tree) reconfiguration times instead of short FDDI wrap times achieved with a concentrator tree architecture.

The management of all devices connected to a shared-media hub is straightforward. The management device can see all of the connected devices given the broadcast nature of the shared media. For switched devices, the management device cannot directly see all of the switched ports. The two common solutions to this problem are port mirroring, where the port monitored is mirrored to a second port to which the management workstation is connected, or implementation

of an RMON 2 agent (or AMON agent for ATM) on the switch which collects management information from all ports and responds to SNMP requests from the management workstation. The port mirroring technique is limited and can monitor only one port at a time. For this reason, implementation of RMON 2 or AMON agent is recommended.

5.2.1.9.2 Virtual LANs and Emulated LANs

Virtual LANs (VLANs) and Emulated LANs (ELANs) provide a means for achieving the broadcast domain isolation of routing while retaining the throughput advantages of layer 2 switching. A VLAN is effectively standard TCP/IP running on top of ATM instead of Ethernet. An ELAN is one of what could be many virtual ATM LANs running on the same physical media. In a VLAN and ELAN environment, a number of vendor frame-tagging methods are not interoperable, and some VLANs may not be definable between multiple switches that are interconnected via a backbone.

5.2.1.9.2.1 Virtual LANs (VLANs)

There are four distinct types of VLANs, not all of which are supported by all vendors:

- VLANs defined by port number on the switch(es)
- VLANs defined by the MAC address of the user devices
- VLANs defined by the IP subnet mask of the user devices
- VLANs created automatically by commonality of IP subnet mask

Currently there are Virtual LAN capabilities being provided by most vendors of LAN switching products. Such Virtual LAN capabilities are intended to prioritize packets and limit broadcast and multicast packet transfers (which can reduce the effectiveness of switching capabilities if sent to all interconnected systems). Future capabilities of VLANs may include network management and security services. IEEE 802 has three efforts on-going to support an interoperable standards based Virtual LAN capability:

- Standard for Local and Metropolitan Area Networks – Supplement to Media Access Control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering (IEEE 801.1p)
- Draft Standard for Virtual Bridged Local Area Networks (IEEE 802.1Q)
- Link-layer Standard for Interoperable LAN Security (SILS) standard (IEEE 802.10)

5.2.1.9.2.2 Emulated LANs (ELANs)

Similar to that provided by VLANs in a conventional LAN environment, emulated LANs (ELANs) provide the ATM environment with a mechanism for isolating traffic and minimizing the propagation of unwanted broadcast messages. In a mixed Ethernet-ATM environment, ELANs and VLANs can be logically associated. A router, or some routing function, is needed to move data between different ELANs or VLANs.

Shipboard networks should provide appropriate VLAN support to embarked forces that meets the need for isolation of ship’s force subnets.

5.2.1.10 Network Components

5.2.1.10.1 Backbone Switches

5.2.1.10.1.1 Ethernet and Fast Ethernet Switches

Network devices that provide switched-Ethernet service fall into the following categories:

- Ethernet to Ethernet,
- Ethernet to Fast Ethernet uplink(s),
- Ethernet to FDDI uplink(s),
- Ethernet to ATM uplink(s),
- Fast Ethernet to Fast Ethernet,
- Fast Ethernet to ATM uplink(s).

Ethernet and Fast Ethernet switches should provide SNMP management support, and should include support of RMON 2. They should support VLANs, including VLANs defined by IP mask address.

5.2.1.10.1.2 FDDI Switches

FDDI switches provide the advantages of bandwidth scaleability when used in a peer-to-peer environment, and rapid switching when setup for cut-through switching. FDDI switches should provide a proxy-ARP (Address Resolution Protocol) function to support the normal ARP process that occurs on a shared-media FDDI ring. Note that loops created by redundant inter-switch paths will be resolved via Spanning Tree protocol, which is a very slow reconfiguration process. Where reconfiguration time must be minimized, use tree-connected FDDI concentrators that reconfigure rapidly using FDDI's SMT wrap protocol.

All FDDI switches should be capable of being managed via RMON2 and SNMP management devices.

5.2.1.10.1.3 ATM Switches

ATM switches should be non-blocking and should provide separate queuing for different QoS classes:

- Constant Bit Rate (CBR)
- Variable Bit Rate – Real Time (VBR-RT)
- Variable Bit Rate – Non Real Time (VBR-NRT)
- Available Bit Rate (ABR)
- Unspecified Bit Rate (UBR)

They should support UNI 3.1 and Phase 1 (or later) PNNI.

All ATM switches have similar cell switching times; however, call setup times vary widely. The calls/second rate of the switches must meet expected requirements.

If LANE Services (LANE Emulation Client Server (LECS), LANE Emulation Server (LES) and Broadcast/Unknown Server (BUS)) are to run on the backbone switches, determine the maximum BUS packet transfer rate (which varies widely among different switch vendors) and verify that it meets the expected requirements. In this context, note that unicast transfers to users whose addresses are not yet cached make use of the BUS services in LANE, so that a low-throughput

BUS can be overloaded even if there is no multicast or broadcast traffic. (If the BUS throughput performance with LANE services running on the backbone switches is inadequate, consider running the services on edge devices or on dedicated LAN Emulation Servers.)

Backbone ATM switches should be procured with dual, hot-swappable power supplies with separate AC power lines, and all line cards should be hot swappable.

All ATM switches used aboard Navy ships should be capable of being managed via RMON 2, AMON and SNMP management devices.

5.2.1.10.2 Edge Devices

Edge devices are needed whenever workstations of one type (e.g., Ethernet) must connect to a backbone of another type (e.g., FDDI or ATM). When edge devices are used in shipboard environments, they should be dual-homed to two different backbone devices for reliability and survivability reasons.

5.2.1.10.3 Modular Versus Fixed-Configuration Hubs

As stated, all backbone switches will be modular. However, edge devices are available in either a modular or fixed configuration option. The fixed configuration, (which consists of a single board with a fixed set of I/O ports), is less expensive than a modular hub but offers no flexibility for changing the interface mix. Where a hub needs to support a variable mixture of Ethernet, Fast Ethernet, FDDI and ATM interfaces, use a modular hub. In installations where a large number of workstations of the same interface type are located, consider use of fixed-configuration hubs to save cost.

5.2.1.10.4 Routers

Routers can be obtained in several configurations:

- Dedicated standalone routers – should be used whenever high-performance routing is needed.
- Routing functionality implemented within a hub and sharing processing power with other hub functions – may be used whenever routing is incidental to the hub function and is not expected to be the throughput bottleneck
- Routing software in workstations – should be avoided because routing is a resource intensive task that is best handled by dedicated hardware that is centralized to simplify network management.

5.2.1.11 Wireless LANs

Wireless LANs are a new but rapidly growing technology. The commercial marketplace is evolving rapidly, and it is difficult to provide stable guidance. The following is provided as near-term guidance, and will be updated as the market matures:

- As breakthroughs in this technology will be market-driven use commercial standards; do not implement wireless LANs using Navy-proprietary solutions.
- Use wireless LANs aboard ship only where mobility is an overriding consideration. Wireless LANs will always provide lower performance at a higher cost than wired LANs. Consider wireless LANs as a backup or mobile extension to a shipboard wired LAN; not

as a substitute for the wired LAN. Wireless LANs offer a potential contingency system to coordinate damage control aboard ships when the cable plant has been damaged.

- Do not use wireless LANs to transfer secure information. Wireless LANs do not provide the degree of security that can be obtained with fiber optic LANs. Information sent over wireless LANs can be intercepted by off-board listeners. Where security features must be added to wireless LANs, do so in a manner that does not result in a proprietary solution. (Encryption in the workstation with standard wireless LAN NICs is preferable to encryption embedded within the wireless LAN protocol.)

5.2.1.11.1 Wireless LAN Standards

The most widely used wireless LAN protocol in the past is the Wireless LAN Interoperability Forum OpenAir 2.4 Specification. The IEEE STD 802.11-1997 Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specification was approved on June 27, 1997. Although it is too early to predict how soon 802.11 wireless LANs will supplant OpenAir wireless LANs in popularity, the near-term guidance of this document is to favor the 802.11 standard over the proprietary OpenAir standard.

However, in spite of the approved IEEE standard, there is no guarantee that wireless LAN components from different vendors will interoperate. The 802.11 standard provides many options:

- Frequency Hopping Spread Spectrum Radio in the 2400-2483.5 MHz band:
  - 1 Mbps operation using 2-level Gaussian Frequency Shift Keying (GFSK)
  - Optional 2 Mbps operation using 4-level GFSK
- Direct Sequence Spread Spectrum Radio in the 2400-2483.5 MHz band:
  - 1 Mbps operation using Differential Binary Phase Shift Keying (DBPSK)
  - 2 Mbps operation using Differential Quadrature Phase Shift Keying (DQPSK)
- Infrared:
  - 1 Mbps using 16-position Pulse Position Modulation (16-PPM)
  - Optional 2 Mbps using 4-position Pulse Position Modulation (4-PPM)

The near-tern guidance for the use of Wireless LANs aboard naval ships is to use the IEEE 802.11 Frequency Hopping Spread Spectrum (FHSS) option at 2 Mbps data rate using 4-level GFSK.

While near-term guidance is to use the IEEE 802.11 FHSS standard, it is not the only non-proprietary wireless LAN standard. In Europe, the Escuela Tecnica Superior de Ingenieros (ETSI) HIPERLAN standard ETS 300 652 is being put forward as a potential worldwide standard. HIPERLAN has the advantage of supporting data rates up to 10 Mbps, but requires a wider bandwidth in a new frequency range around 5 GHz. Until recently, this band was illegal for use in the United States; however, on January 9, 1997 the FCC allocated 300 MHz of spectrum in the same band as HIPERLAN uses, thereby opening the possibility of 10 Mbps HIPERLAN wireless LANs in the near future. The use of HIPERLAN should be postponed pending its standardization within the U.S.

There is also work underway within the ATM Forum to develop a Wireless ATM standard; however, widespread use of wireless ATM should be postponed pending approval of the associated standards.

5.2.2 Wide and Metropolitan Area Network Physical and Data Link Layer Technologies

Best Practices

WAN services should be obtained through the Defense Information Systems Network (DISN). Internet services should be provided through Information Technology Service Centers (ITSCs) where required security measures can be provided. Wide area native ATM services should be preferably obtained from DISA. Where DISA service is not available or does not meet the price performance requirements, commercial ATM services can be used. ISDN is recommended for quick implementation of VTC services.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Commercial Internet Service Providers OpenAir 2.4 Wireless	DISN for IP Service DISA ATM Service (DAS) or Commercial ATM Service ISDN	DISN for IP Service DISA ATM Service (DAS) or Commercial ATM Service ISDN	DISN for IP Service DISA ATM Service (DAS) or Commercial ATM Service ISDN	DISN for IP Service DISA ATM Service (DAS)	IEEE STD 802.11-1997 Wireless xDSL
Activities, Platforms, Operational Environments		Shore			

Table 5-3. Physical and Data Link Recommended Implementations for WANs

5.2.2.1 Local Loop

The local loop is traditionally defined to be under the control of a local telephone company. This is the service provided between the Local Exchange Carrier (LEC) and the customer. (The term “local loop” originated from the fact that a standard two-wire Plain Old Telephone System (POTS) line is really a loop from the Central Office to the off-hook telephone and back to the Central Office.)

While such services are usually provided by the LEC, users on large installations who own their own “local loops” can use this technology as well. While this technology is not the preferred choice to extend one’s network, certain applications may benefit from these techniques. To repeat an earlier example, a remote guard shack 2 miles from the nearest network connection may need a multi-Mbps circuit for a camera and/or monitor. The cost to run fiber may be too prohibitive whereas an existing POTS line with the proper equipment may be adequate.

5.2.2.2 Digital Subscriber Line

Several closely related products known as xDSL (ADSL, RADSL, HDSL, SDSL, etc.) are designed to provide Mbps types of point-to-point communications over 1-3 mile copper segments (indeed, many telephone company DS-1 connections are really HDSL underneath but the handoff to the customer is DS-1). They use the higher frequencies that are normally filtered out in the telephone system by the 3kHz bandpass filters (commonly known as voice coils) for which telephone modems are forced to compensate. DSL products are useful for router-router, router-end system or end system-switch situations where it is important to salvage existing copper pairs and the copper run does not exceed the supported distances. This makes the technology attractive to sprawling bases or garrisons where the command owns the copper plant (and can remove the voice coils that prevent DSL technology from working). Because of the plethora of technologies, both ends of a DSL link should be purchased from the same, or guaranteed interoperable pair of, vendors. DSL technology should not be used in new installations where fiber optic cable plants should be installed.

5.2.2.3 ISDN

Integrated Services Digital Network (ISDN) is available in DON from either commercial off base providers or from a government owned or leased on-base switch network. ISDN is used for switched voice, data and video applications. The most prevalent application is for Video Teleconferencing where dedicated transmission is not cost effective. The majority of Navy (and DOD) shore VTC systems use ISDN as the transport media. ISDN is widely available in the continental US, Japan and Europe and is generally ordered in one of two transmission service types:

1. ISDN Primary Rate Interface (also known as PRI 23B+D service - 23 Bearer 64Kbps channels.

2. 1 Delta 64Kbps signal channel delivered from the telephone company on 4-wires) or ISDN Basic Rate Service (also known as BRI 2B+D – 2 Bearer 64Kbps channels and 1 64Kbps Delta channel delivered from the telephone company on 2-wires).

Especially well suited for geographically separated VTC users, ISDN delivers a cost effective usage based transmission service that allows for instant H.320 video calls on demand anywhere and anytime.

The following policy, guidelines and key factors for success should be followed if implementation of ISDN is required.

Best Practices

ATM is preferred as a WAN/MAN protocol over ISDN. However, if ATM is unavailable and ISDN is required to support VTC and low speed data connectivity, procure ISDN capable of Bearer Capability – CSD (Circuit Switched Data) 64Kbps Unrestricted Digital Information (UDI) also called “clear channel”.

- IMUX Capability – For data calls at rates above 128Kbps (i.e. 224, 256, 336 or 384Kbps) Bandwidth On Demand Interoperability Group (BONDING) Mode 1 multiplexing should be employed (see FIPS Pub 178). Note: When calls are originating and terminating on PRI service H0 (i.e. H0 384Kbps switched calls) preferred due to the guaranteed single

end to end clock source. End to end Local Exchange Carrier (LEC) - International Exchange Carrier (IXC) and IXC-LEC delivery capability is a problem with implementing this service – not all Regional Bell Operating Companies (RBOC) LEC and IXC companies are provisioned to handle this service due to present trunking and switch configuration schemes.
- National ISDN 1 - Customer Premise Equipment (CPE) must be NI1 compliant.

Guidelines

In planning any ISDN network several key items need to be taken into consideration:

- Who do you plan to communicate (VTC) with and what type of transmission service do they possess? If possible, order ISDN service with the same Inter-exchange Carrier (IXC) (AT&T or FTS-2000 etc.).
- What data rate is your VTC equipment capable of (128, 384 or 768Kbps)? Order ISDN service to match the highest data rate of your equipment or at least those of your distant end (i.e. single BRI for 128Kbps for desktop VTC as a minimum and Tri-BRI 384Kbps service (or PRI) for cart and room systems).
- What is the Concept of Operations for your VTC Network? If you plan to call OCONUS sites you will need to be PIC commercial ISDN IXC as your primary carrier, or if the majority of your distant end sites are FTS-2000 (FTS-2000 = 10387) you will want to order VON (Virtual Off Net) service from a commercial Carrier (i.e. AT&T Accunet =10288, MCI = 10222, Sprint = 10333). Note: Effective June 98 the FCC will be introducing the 7 digit PIC code (i.e. the new long distance carrier code for AT&T will be 1010288) IAW FCC rule 3DEC97 DA972528.TXT. Take note of this change and be prepared to modify ISDN access switch parameters (i.e. dial string - outgoing qualifiers) as required.
- How Many and What Type ISDN Drops Are Required? Should your plans require multiple (4 or more) dedicated BRI drops for locally distributed desktop VTC units, you may consider ordering a single PRI from the LEC and terminating it into an Inverse Multiplexer (i.e. Teleos Model 20 or Model 60) to distribute your own BRI S/T interface directly to the desktop. This local distribution method requires the use of Category 5 UTP wire from the IMUX to the desktop video terminals.
- For medium to large campus type ISDN distributed networks in which PRI and or multiple BRI's are employed, it is recommended that the Inverse Muliplexer (i.e. Teleos Model 60 or 200 Access Switch) be equipped with Q.921 and Q.931 protocol monitoring capability. The equipment should be capable of monitoring the status of Layer 1 physical (I.430), Layer 2 Link (Q.921) and Layer 3 Network (Q.931) protocols. This recommendation is made in order to aid the expediting of fault isolation (layer 2 and 3 debug) efforts.

Key Factors For Success

- ISDN Directory Numbers (DN's) – Ensure accuracy
- ISDN Service Profile Identifiers (SPIDs) – Ensure accuracy
- ISDN Switch Type (i.e. AT&T 5ESS, DMS-100 or Erricson) – Know the type switch you are connecting to and program your CPE (i.e., Terminal adapter or Inverse multiplexer) accordingly.
- ISDN Switch Software (i.e. NI-1 or Custom) – Again, know the type switch you are connecting to and program your CPE (i.e. Terminal adapter or Inverse multiplexer) accordingly.

- ISDN Capability Package – BRI's orders should specify V/C (V - voice and C – circuit switched data) for each B channel and P (Basic D Channel Packet) for the Delta Channel.
- ISDN NT1 (Network Termination 1 Device) Distance Consideration: The LEC (Local Exchange Carrier) will generally deliver a BRI U loop up to 18K' from the servicing Central Office (C/O) – when extending your U loop (in house) pay close attention to the length of your run to ensure it does not exceed 18K' in overall length. If in doubt contact your Telco to obtain BRI U length from the C/O to the LEC demarcation point on the premises.

5.2.2.4 Trunking

WAN connections originally consisted of 56 (or 64) Kbps circuits. These were increased to 1.5 Mbps DS-1 service (formerly called T-1) and 45 Mbps DS-3 service (formerly called T-3). Today's dedicated circuits can reach 155 Mbps (OC-3). The costs for these high-speed circuits is dramatically high (in some cases $500,000.00 per year for a single circuit connecting two sites). A number of methods can be used to cut this cost. First, DISA is standing up a high-speed CONUS network as part of the DISN (Defense Information Systems Network). Second, one can procure ATM services from DISA or a commercial carrier specifying both peak and sustained data rates. Usage above this rate is metered. Use of the Secret Internet Protocol Routing Network (SIPRNET) and the Non-classified Internet Protocol Routing Network (NIPRNET) is mandated for joint interoperability. The regional ITSCs will provide connectivity to the public Internet.

5.2.3 Radio Communications to Dispersed Forces

Best Practices

To participate in multi-media driven collaborative planning, and decision support operations, underway ships and deployed MEUs need a minimum standard data rate of 128 kbps during operations. This data rate is not yet economically achievable. Continued research, development, and acquisition should be sustained to attain this data rate. It is preferred that multiple independent communications paths be used for maximum fault tolerance. All media and all information classifications should be aggregated using appropriate technologies for multiplexing and encryption. Transitions between satellite footprints, between Line-of-Sight and SATCOM, from afloat to ashore, and from embarked to disembarked should be seamless.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
INMARSAT A, M	UHF SATCOM SHF SATCOM EHF SATCOM GBS ATS INMARSAT B, C UHF LOS	UHF SATCOM SHF SATCOM EHF SATCOM GBS ATS INMARSAT B, C UHF LOS	UHF SATCOM SHF SATCOM EHF SATCOM GBS ATS INMARSAT B UHF LOS	UHF SATCOM SHF SATCOM EHF SATCOM GBS ATS INMARSAT B UHF LOS	Globalstar Iridium Orbcom Teledesic
Activities, Platforms, Operational Environments		Ship, Ground, ITSC			

Table 5-4. Physical and Data Link Recommended Implementations for Radio Communications to Dispersed Forces

The Naval Service is dependent upon exterior RF communication to maintain connectivity between its ashore, afloat and airborne command sites. RF links are also required to maintain coordination between the command sites and afloat tactical units. Standards exist for most military RF communications channels. Commercial RF communication channels often possess proprietary over-the-air interface standards, which prevent communication between equipment from different vendors. The Navy is developing internal standards for the transfers of high-speed data over radio WANs. Issues being addressed include data flow control, the termination of data delivery time, and prioritizing of data for delivery. Two such developments are the Afloat Telecommunications System (ATS) and Automated Digital Network System (ADNS). ADNS passes Internet Protocol (IP) datagrams, including multicast and router-to-router protocols.

Figure 5-6 is provided to illustrate the relationships between the various RF communication bands.

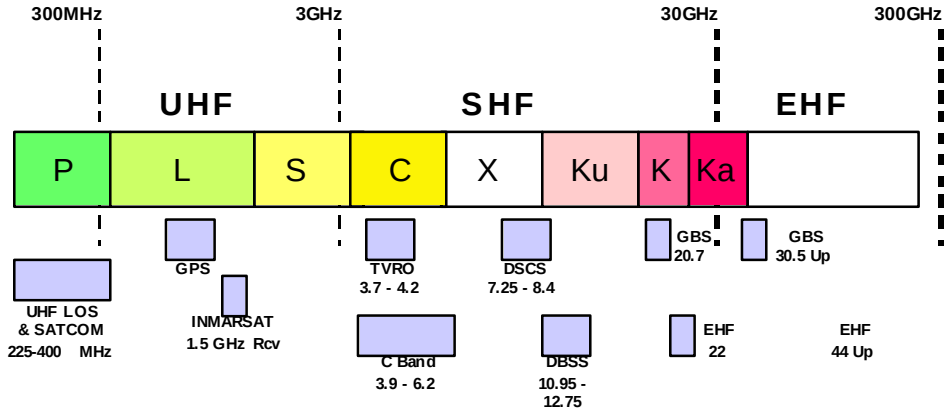


Figure 5-6. RF Bands Used in SATCOM

5.2.3.1 Military Satellite Communication (MILSATCOM)

MILSATCOM systems include those systems owned or leased and operated by the DoD. The basic elements of satellite communication consist of a space segment, control segment, and a terminal segment (air, ship, ground, etc.). An implementation of a typical satellite link will require the use of satellite terminals, user communication extension, and the use of military or commercial satellite resources.

The Navy UHF SATCOM System provides communication links, via satellites, between designated mobile units and shore sites. These links supply worldwide coverage between the latitudes of 70 degrees north and 70 degrees south. Multiple satellite constellations are currently in use: Fleet Satellite Communications System (FLTSATCOM), Leased Satellite (LEASAT), and the current series UHF Follow-On (UFO). The SATCOM system includes satellites, RF terminals, subscriber subsystems, personnel, training, documentation, and logistic support. The Navy SHF SATCOM system provides a high-capacity and jam resistant, full-duplex communication capability for high-value Naval combatants, special purpose ships, and selected shore sites. Defense Satellite Communication System Phase II (DSCS II) satellites and a second constellation of DSCS III satellites are currently being used for Navy SHF satellite communication. The Milstar satellite communication system is designed to meet the projected minimum essential wartime requirement associated with military communication. The system is survivable and jam resistant with Low-Probability-of-Intercept (LPI) and relay functions to meet strategic, tactical, and other associated communication needs. Block I satellites have growth capability via the Block II upgrade.

5.2.3.1.1 Ultra High Frequency (UHF) Satellite Terminal Standards

Data and voice services are provided to the Navy via multiple services, 5 kHz, 25 kHz and 500 kHz transponder channels. One of the 25 kHz channels is used for broadcast purposes only. The remaining channels provide simplex communication within the technical limitations of the channel bandwidth. Navy UHF satellite communication is used to carry tactical communication traffic to and from the fleet. Approved crypto is required to secure all RF links and measures are taken to prevent hostile analysis.

5.2.3.1.1.1 5kHz and 25 kHz Service

For 5 kHz or 25 kHz single channel access service supporting the transmission of either voice or data, the following standard is mandated:

- MIL-STD-188-181A, Interoperability Standard for Single Access 5 kHz and 25 kHz UHF Satellite Communications Channels, 31 March 1997.

5.2.3.1.1.2 5kHz Demand Assigned Multiple Access (DAMA) Service

For 5 kHz DAMA service, supporting the transmission of data at 75-2400 bps and digitized voice at 2400 bps, the following standard is mandated:

- MIL-STD-188-182A, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 31 March 1997.

5.2.3.1.1.3 25kHz Time Division Multiple Access (TDMA)/Demand Assigned Multiple Access (DAMA) Service

For 25 kHz TDMA/DAMA service, supporting the transmission of voice at 2400, 4800, or 16000 bps and data at rates of 75-16000 bps, the following standard is mandated:

- MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, dated 2 December 1996.

5.2.3.1.1.4 Data Control Waveform

For interoperable waveform for data controllers used to operate over single access 5 kHz and 25 kHz UHF SATCOM channels, the following standard is mandated to provide a robust link protocol that can transfer error free data efficiently and effectively over channels that have high error rates:

- MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993.

5.2.3.1.1.5 DAMA Control System

For the minimum mandatory interface requirements for equipment that control access to DAMA UHF 5 kHz and 25 kHz MILSATCOM channels, the following standard is mandated:

- MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996.

5.2.3.1.2 Super High Frequency (SHF) Satellite Terminal Standards

Communication services are provided via Earth, spot, and multi-beam array antennas. Data and voice services related to national military communication needs are carried via transponder channels. The six channels per DSCS III satellite vary in RF bandwidth from 50 to 85 MHz. Navy SHF satellite communication is used to carry tactical and strategic communication traffic to and from the fleet. Approved crypto is required to secure all RF links and measures are taken to prevent hostile analysis. The OM-55 modem is being phased out. The OM-73 and CQM-248A modems are the current technology. The Universal Modem System (UMS) is scheduled for Fleet Operational Test and Evaluation (FOT&E) in April 2000. The UMS offers the Navy a choice of Low Data Rate (LDR), up to 19.2 Kbps FSK and Medium Data Rate (MDR), 16 Kbps to 8.472 Mbps PSK service. Additional features include: the ability to use commercial satellites (C- and Ku-band), Frequency Division Multiple Access (FDMA), automatic RF power control, centralized control of UMS networks, and Over the Air Rekey (OTAR). Scheduled installations include command platforms, SHF SATCOM activities, Army, Air Force, United Kingdom and other NATO sites for extended interoperability.

Access http://www.jmcoms.org for more information about the Navy's SATCOM equipment development efforts.

5.2.3.1.2.1 Satellite Terminal Standards

To support minimum Radio Frequency (RF) and Intermediate Frequency (IF) requirements and ensure interoperability of SATCOM earth terminals operating over C-, X-, and Ku- band channels, the following standard is mandated:

- MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995.

Current draft standards for MILSATCOM are:

- MIL-STD-188-166 (Interface Standard, Interoperability and Performance of Non-Electronic Protective Measures (EPM) for SHF SATCOM Link Control Protocols and Messaging Standards),

- MIL-STD-188-167 (Interface Standard, Message Format for SHF SATCOM Demand Assignment), and
- MIL-STD-188-168 (Interface Standard, Interoperability and Performance Standards for SHF Satellite Communications multiplexors and Demultiplexers).

5.2.3.1.2.2 Phase Shift Keying (PSK) Modems

For minimum mandatory requirements to ensure interoperability of PSK modems operating in Frequency Division Multiple Access mode, the following standard is mandated:

- MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995.

5.2.3.1.3 Extremely High Frequency (EHF) Satellite Payload and Terminal Standards

World wide data and voice services are provided via two modes. Block I satellites offer Low Data Rate (LDR) service as follows. Low Hop Rate (LHR) at 75, 150, and 300 bps. High Hop Rate (HHR) provides 75 to 2400 bps data and 2400 bps voice service. Block II satellites add a Medium Data Rate (MDR) service, exchanging data at 4.8 Kbps to 1.544 Mbps. Navy EHF satellite communication is used to carry minimum essential communication traffic to and from the fleet. All RF links are secured by approved crypto. The system offers both jam resistance and LPI.

5.2.3.1.3.1 Low Data Rate (LDR) Links

For waveform, signal processing, and protocol requirements for acquisition, access control, and communication for low data rate (75-2400 bps) EHF satellite data links, the following standard is mandated:

- MIL-STD-1582D, EHF LDR Unlinks and Downlinks, September 30, 1996; with Notice of Change 1, dated 14 February 1997.

5.2.3.1.3.2 Medium Data Rate (MDR) Links

For waveform, signal processing, and protocol requirements for acquisition, access control, and communication for medium data rate (4.8 Kbps - 1.544 Mbps) EHF satellite data links, the following standard is mandated:

- MIL-STD-188-136, EHF MDR Uplinks and Downlinks, August 26, 1995; with Notice of Change 1, dated August 15, 1996, and Notice of Change 2, dated 14 February 1997.

5.2.3.1.4 Global Broadcast System (GBS)

Standards for GBS integration into the DISN have not been finalized, however proposals are in progress. GBS is patterned after Direct Broadcast Satellite (DBS), which is an example of Ku-band service concentrated in the more populated and affluent terrestrial areas of the Earth. It is a one-way broadcast that uses powerful uplink channels to make enough link budget that receivers (and antennae) can be quite small – approximately 18".

5.2.3.2 Commercial SATCOM

Terrestrial commercial carriers such as International Telecommunication Satellites (INTELSAT), Hughes Communication Services, and Orion, provide communication coverage for most sites on the Earth. Coverage by Earth coverage beams exists worldwide. Many carriers can provide higher

RF gain zone and spot coverage beams for most terrestrial sites. The higher RF gain allows the Earth terminal antenna to be smaller than that required for the same class of service in an Earth coverage RF beam. Both C- and Ku-band service are available world wide, but the Ku-band service is directed to service more populated terrestrial regions. The newest class of service, Direct Broadcast Satellite (DBS), is an example of Ku-band service concentrated in the more populated and affluent terrestrial areas of the Earth. Commercial carriers are capable of transferring many forms of data and protocol stacks by using proprietary protocols internal to the RF link. The transmit and receive sites perform the task of insuring continuity and delivery of the subject data.

The service provided is typically point-to-point and can be integrated by use of Point-to-Point Protocol (PPP) as a router-to-router interconnect. It is recommended that these channels be considered for integration after careful analysis of security.

The Commercial Satellite Communications Initiative (CSCI) has examined the vulnerabilities of using commercial satellites for military purposes. Currently completed studies include:

- “Project STARCROSS Commercial Satellite Vulnerability Study (U)”, Report No. GX/S-733-93 of September 1993 for fixed and mobile satellite service provided by COMSAT, Hughes, and Loral Space Systems.
- “Project STARCROSS Mobile Satellite System Assessment: Phase II Results (U)”, APL/TSD 34011 of December 1996 for mobile satellite service provided by Iridium.
- “Project STARCROSS Mobile Satellite System Assessment: Phase III Results (U)”, APL/TSD 34672 of November 1997 for mobile satellite service provided by Globalstar

For release of documents, contact: Commander Naval Information Warfare Activity, 9800 Savage Road, Fort George Meade, MD 20755-6000

5.2.3.2.1 International Maritime Satellite (INMARSAT)

Since 1982 the International Maritime Satellite Organization (INMARSAT) has provided RF communication service to ocean regions and mobile users. The charter is to provide ship-to-shore and shore-to-ship telex and telephony for maritime customers, but recently land-mobile and air platforms have been added to the service.

INMARSAT system does not offer any communication protection and international treaty limits its use for purposes of war. According to an INMARSAT Consortium ruling (INMARSAT letter L303.0/vN/jr5376L of 8 November 1994), military use not involving armed conflict or any threat to or breach of peace is permitted. Also, military use of INMARSAT by UN peacekeeping or peacemaking forces acting under the auspices of the UN Security Council is permitted, even if engaged in armed conflict.

INMARSAT-B is the mandatory format for voice and data transfer. INMARSAT-C is used for Coast Guard navigation aides, as required. (Other INMARSAT systems are not recommended. INMARSAT-A is an expiring standard and is too easily compromised. INMARSAT-M lacks the communication quality offered by INMARSAT-B. Navigation aids via INMARSAT-C may become redundant by the year 2000.)

INMARSAT-B’s internal link format is proprietary to INMARSAT which produces an effective data rate of 56 Kbps. The INMARSAT system does not offer any communication protection. Terminal manufacturers market terminals capable of operating in all existing INMARSAT environments. COMSAT Corp. in Clarksburg, MD at 301-428-2549, 2391, or 2660 has a current

list of certified INMARSAT terminal vendors. The information is also available via the World Wide Web at http://www.inmarsat.org/.

5.2.3.2.2 High Bandwidth Commercial SATCOM

The above-identified maritime transponders are not capable of a data transfer rate greater than 56 Kbps. Though high data rate service has been demonstrated from ships via terrestrial satellite carriers such as COMSAT, Hughes, and Orion no standards are currently designated. All demonstrations have been conducted close to terrestrial sites where high data rate service is offered, versus the middle of an ocean where the service is ultimately desired. As with any other installation of new equipment aboard a ship, a principle concern is location of the new above deck antenna(s).

5.2.3.2.3 Ku-Band Service

Data rates greater than 56 Kbps, as provided by INMARSAT L-band, are provided by terrestrial satellite service using C- and Ku-band RF links. Data transfer rates up to full motion video and beyond are capable within the satellite RF beam coverage foot print of the satellite. The issue of RF beam coverage is a principle issue relative to where this class of high data rate coverage is available.

High data rate service is often provided in 64 Kbps increments. Data-rates of 256 Kbps, 384 kbps, T1, E1, and 2.048 Mbps are popular transfer data rates. An Earth antenna as small as 2.4m is capable of receiving 24 Mbps data. Newer satellites transmitting to very small aperture terminal (VSAT) equipment with 18” diameter, receive-only antenna are capable of data-rates as high as 400 Kbps with average data transfer rates of 200 Kbps.

Four vendors of mobile satellite service use Low Earth Orbit (LEO) as this decreases the distance between uplink, satellite, and downlink stations with respect to geosynchronous satellites, enabling vehicle-mounted and handheld antennae as well as higher information transfer rates. Three of these vendors are considered “Big” because of the number of satellites in their constellations. The number of orbits of these satellites directly results in higher throughput capability as well as greater satellite coverage of the earth.

> **Globalstar** is a constellation of bent-pipe satellites being launched by a consortium of Loral and Qualcomm. The system is known as a Big LEO system, is licensed by the Federal Communications Commission (FCC). Bent pipe means that the earth station (entry into the backbone network) and the mobile user must both be under the satellite footprint. The number of satellites and orbital configuration is such that satellites should be above the horizon at all times in temperate and equatorial areas (Globalstar does not provide polar coverage). Because Globalstar was designed with trunked voice applications in mind, media access is point-to-point at rates of approximately 19.2 Kbps (Rate Set 2), 9.6 Kbps, 4.8 Kbps and 2.4 Kbps. The user is provided a handset similar to that in any telephone cellular system. Predicted weight is 16 oz with a desired lifetime of 24 hours standby-time and 2 hours talk-time.
>
> **Iridium** is a constellation of satellites with crosslinks that is being launched by a consortium led by Motorola. This system is known as a Big LEO and is licensed by the FCC. With satellite crosslinks, the mobile user and terrestrial network entry can be anywhere. Iridium's orbital configuration is near-polar so complete global coverage (including Polar Regions) can be expected. Because Iridium was designed with trunked voice applications in mind,

media access is point-to-point at rates of approximately 9.6 Kbps. The user is provided a handset similar to that in any telephone cellular system. Predicted weight is 16 oz with a desired lifetime of 24 hours standby-time and 2 hours talk-time.

Orbcomm is a constellation of satellites launched by Orbital Sciences Corporation. This system is known as a Little LEO and is licensed by the FCC. It is a data-only, store-and-forward system designed to relay small e-mail messages from users to e-mail gateways, for dispatch into the Internet. The mobile user is provided an antenna and module that connect to a host computer via RS-232. Demonstrated systems have been designed for automobile installation and weigh less than 5 pounds complete.

Teledesic is an emerging infrastructure of satellites expected to reach initial operational capability in 2002. It is a consortium with support from AT&T, McCaw and Microsoft. The 288 satellites are planned into a near-polar low earth orbit, so complete earth coverage, including Polar Regions, can be expected. Teledesic has satellite crosslinks, and an order of magnitude higher capacity than the other big LEOs. While the interface to the terrestrial internet is as yet undefined, the term 'Internet' appears prominently in Teledesic's business plan. Teledesic plans to develop alliances with service provider partners in host countries worldwide, rather than marketing directly to end users. The Teledesic system is designed to provide up to 64 Mbps on the downlink and up to 2 Mbps on the uplink. Broadband terminals will offer 64 Mbps of two-way capacity. Teledesic plans to be operational by the year 2002.

5.2.3.3 Line-of-Sight (LOS) Radio Communications

5.2.3.3.1 Military Communication Systems

5.2.3.3.1.1 High Frequency (HF) and Automatic Link Establishment (ALE)

For both ALE and radio subsystem requirements operating in the HF bands, the following standard is mandated:

- MIL-STD-188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard, September 15, 1988; with Notice of Change 1, dated 17 June 1992, and Notice of Change 2, dated 10 September 1993.

5.2.3.3.1.1.1 Anti-jamming Capability

For anti-jamming capabilities for HF radio equipment, the following standard is mandated:

- MIL-STD-188-148A, Interoperability Standard for Anti-Jam Communications in the HF Band (2-30 MHz), 18 March 1992.

5.2.3.3.1.1.2 Data Modems

For HF data modem interfaces, the following standard is mandated:

- MIL-STD-188-ll0A, Data Modems, Interoperability and Performance Standards, 30 September 1991.

5.2.3.3.1.2 Very High Frequency (VHF)

For radio subsystem requirements operating in the VHF frequency bands, the following standard is mandated:

- MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985.

5.2.3.3.1.3 Ultra High Frequency (UHF)

For radio subsystem requirements operating in the UHF frequency bands, the following standard is mandated:

- MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, 15 March 1989.

5.2.3.3.1.3.1 Anti-jamming Capability

For anti-jamming capabilities for UHF radio equipment, the following standard is mandated:

- STANAG 4246, Edition 2, HAVE QUICK UHF Secure and Jam-resistant Communications Equipment, June 17, 1987; with Amendment 3, dated August 1991.

5.2.3.3.1.4 Super High Frequency (SHF)

For radio subsystem requirements operating in the SHF frequency bands, the following standard is mandated:

- MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 7 May 1987; with Notice of Change 1, dated 28 July 1992.

5.2.3.3.2 Commercial Non-Satellite Radio Communication Systems

5.2.3.3.2.1 Personal Communications Services (PCS)

PCS will support both terminal mobility and personal mobility. Personal mobility allows users of telecommunication services to gain access to these services from any convenient terminal with which they choose to associate themselves. To support personal mobility, the network must be able to distinguish between terminal and personal identifiers; to keep track of current user-terminal associations, user locations, services authorized to the user, and service capabilities of the terminals. Either wireline or wireless terminals may provide personal mobility. Terminal mobility is based on wireless access to the Public Switched Telephone Networks (PSTN). Wireless access standards will govern the protocols and procedures for establishing connections among mobile terminals and between them and fixed terminals of a switched network (or mobile terminals of a different cellular system). IS-41, the current standard within the United States, provides this capability and is compatible with the existing signaling and numbering schemes used in the PSTN.

5.2.3.3.2.2 Mobile Cellular Communications

Mobile cellular radio can be regarded as an early form of “personal communications service.” It allows subscribers to place and receive telephone calls over the PSTN wherever cellular service is provided. Two methods for digital access have emerged, TDMA, and Code Division Multiple Access (CDMA). In North America the standards for TDMA and CDMA are IS-54 and IS-95. Both of these standards use IS-41 as the standard signaling protocol.

5.2.3.3.2.3 Future Public Land Mobile Telecommunications Systems (FPLMTS) standards

The ITU is now working on a third-generation standard for FPLMTS. The aim of this effort is to achieve better compatibility among the various cellular systems such that, by the beginning of the next century, universal global access supporting terminal mobility becomes a reality. The

document now emerging from this effort shall be used as guidance for implementing global terminal mobility.

5.3 Internetwork Protocols

Layers 3 and 4 of the OSI Reference Model (Figure 5-7. ISO/OSI Model Layers 3 and 4) describe the network and transport layers, respectively. Transmission Control Protocol/Internet Protocol (TCP/IP) (defined later) falls into this area. There is currently an active debate within the industry on whether to strictly follow the traditional Internet model in which all data is broken into connectionless packets (called “datagrams”) or allow for connection-oriented streams as in ATM (defined below).

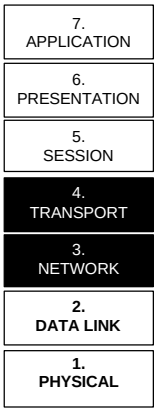


Figure 5-7. ISO/OSI Model Layers 3 and 4

When following the connectionless model, each datagram is handled independently. A decision on how to route information from one point to another is made on each and every datagram. The benefits are that one can be completely independent of the data link layer from one segment to another as packets cross the network. Also, as intermediate links come and go, the independent routing of each datagram provides a good chance that an alternate path will be found on the fly. The disadvantage is that processing, sometimes significant, must occur on each and every datagram, i.e., the “n”th datagram has no knowledge of the path that the “n-1”st datagram took.

The connection-oriented, or “virtual circuit” model requires that one establish a virtual circuit between two points via a call-setup procedure. Once the circuit is created, information can flow along this predefined path without the need to examine the individual data elements. Each virtual circuit can be created with its own quality-of-service requirements (bandwidth, minimum delay, bumping priority, etc.) By allowing a connection-oriented “virtual circuit”, one can pay the processing overhead once in performing the “call setup” to establish the path, then have all subsequent data follow the original path with minimal processing, i.e., higher bandwidth. A disadvantage is that one must recreate the virtual circuit upon any given link failure.

A crude analogy can be made between postal mail and a telephone call. With the postal mail example, a data set too large to fit into one envelope can be broken up into many, separately addressed envelopes (connectionless datagrams). Each envelope can then be transported by independent means from the source to the destination. If, however, a phone call were placed (connection-oriented virtual circuits), the data would travel the same deterministic path from the source to the destination.

This arguments of this debate are much more complex than the above and are beyond the scope of this document. The most likely outcome will be a hybrid set of standards that allow for both environments. One of the major goals of this chapter is to provide a single core infrastructure that will handle both types of data flow. Provisions are made for both implementations to simultaneously exist and pass data back and forth. For example, a low-end client connected to an Ethernet segment generating IP datagrams should be able to simultaneously communicate with a peer operating in the same state as well as with a server that is directly connected to other servers via ATM. Also, a real-time data stream (such as a VTC session or video broadcast) that does not implement IP will be able to share the same core backbone.

Best Practices

ATM from the desktop through the WAN is recommended to the extent that application interoperability and cost will allow. Where ATM is not yet feasible, continued use of Transmission Control Protocol/Internet Protocol (TCP/IP) is recommended for shared media networks (LANs) Point-to-Point (PPP) protocol is recommended for point-to-point links and WANs.

LAN configurations for the backbone, servers, mission critical appliances, and non-mission critical appliances should be consistent throughout the information system domain. Mixing of different protocols on like architectural components (e.g., all non-critical appliances) is not permitted except temporarily during the migration to an advanced protocol.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Novell's IPX	ATM	ATM	ATM	ATM	IPv6
Banyan's Vines	IPv4	IPv4	IPv4	IPv4	
AppleTalk	TCP	TCP	TCP	TCP	
DecNET/LAT	ppp	ppp	ppp	ppp	
Activities, Platforms, Operational Environments		All. ITSC managed			

Table 5-5. Network and Transport Layer Recommended Implementations

5.3.1 ATM

Asynchronous Transfer Mode (ATM) is a connection-oriented transport protocol that collapses many of the layers of the OSI model.

Briefly, ATM uses "virtual circuits". (The virtual circuits can be established in advance (Permanent Virtual Circuits, or PVCs) or dynamically on demand (Switched Virtual Circuits, or SVCs).) ATM Virtual Circuits (VCs) are based on the concept of Asynchronous Time Division Multiplexing, ATDM. Unlike traditional TDM systems in which each multiplexed VC is given a predetermined time slot, ATDM fills the "next" available time slot with data from the "next" available VC. For example, given "n" VCs, traditional TDM would uniformly transmit one fixed-length data unit (called a "cell") from one VC to the next. After one time period, the first cell of all "n" VCs would have been transmitted. If no cells were ready from a particular VC, a "null" cell would be inserted into the multiplexed output stream. (The receiving device would properly identify these "null" cells and discard them.) With ATDM, however, the next cell could come from any VC. For example, if there were two VCs, one of which had twice the bandwidth on the other, then the higher-bandwidth VC would transmit two cells for every cell of the lower-bandwidth VC. Also, if a higher-priority VC had a cell ready, it would be transmitted before a lower-priority VC – even if the former was at a lower bandwidth.

ATM Virtual Circuits can support a number of service classes based on the traffic type, each with an associated set of Quality of Service (QoS) parameters. Example service classes are as follows:

- Constant Bit Rate (CBR), used for circuit emulation and flows which have a constant data rate
- Variable Bit Rate (VBR) for flows which are bursty in nature (further QoS parameters for this traffic type are Peak Cell Rate (PCR) for maximum burst rate and Sustained Cell Rate (SCR) for average rate)
- Available Bit Rate (ABR) for flows which dynamically negotiate their PCR and SCR values
- Unspecified Bit Rate (UBR) for "best-effort" service.

Some applications are obviously linked to particular service class. A 64 Kbps voice circuit is best carried as a CBR stream but voice which is compressed and has silence-suppression enabled can either be VBR or UBR, depending on the robustness of the algorithm. How applications map to the different service classes is evolving.

By allowing VC cells to enter the multiplexed stream under individually controllable conditions, i.e., service classes, one could enforce the QoS for a particular VC. A high-bandwidth VC would have more access to a trunk than a lower-bandwidth VC. Similarly, a high-priority VC has head-of-the-line privileges over a lower-priority VC.

ATM has no length or time-delay constraints. As a result, it is applicable to the LAN as well as the WAN. Further, ATM is a technology that can cut through many of the OSI layers. At the application layer, one could open a virtual circuit between two workstations using all layers of the OSI 7-layer model. Once the circuit was established, however, data could simply flow from the application (layer 7) to the data link layer (layer 2) – without passing through the intermediate layers (3 through 6). (In IP, all data is broken into datagrams, each of which passes through all layers.) ATM can simultaneously support applications whose data does not easily fit the 7-layer model (VTC, voice, real-time data streams, etc.). Finally, VC cells can be replicated at convenient points along the network and sent to multiple users. A single source can transmit one stream to multiple users. If the users are a significant distance apart, say across the country, the stream is not duplicated until the last possible point. This is very efficient in bandwidth utilization, especially for multicast.

For the above reasons, ATM is a technology that must be considered in future systems. It continues to gain acceptance in WAN technology and can offer hundreds and thousands of Mbps rates in the LAN.

As a transition phase, most computer applications implement IP over ATM as opposed to TCP over ATM (IP and TCP are discussed below). As a result, many of today's applications create datagrams within the operating system and transmit those individual datagrams via ATM. As applications' needs warrant, they can be migrated over to ATM such that many of the OSI layers are never traversed, resulting in higher efficiency.

5.3.2 Network Layer

This section provides a discussion of the Network Layer as defined by the OSI Reference Model. The network layer provides the interface between the lower layer protocols and the transport layer protocols and the means for concatenating multiple network segments into a seamless whole. The recommended network layer protocol is the Internet Protocol or IP. This section also addresses protocols that support and integrate IP with the lower layer protocols.

Needs:

- Each protocol that runs over a network requires overhead. This overhead is most commonly manifested in terms of bandwidth used (e.g. to pass routing table updates) and in terms of administrative time and expense. This set of standards is intended to converge to a single set of protocols that exacts this overhead tax but once.
- The IP protocol base outlined here allows one option towards a forward evolution to a multicast set of protocols as they develop in the industry.

5.3.2.1 Internet Protocol

The Internet Protocol (IP), also referred to as the Internet Protocol Version 4 (IPv4), refers to an unreliable, connectionless, datagram service. The IP is defined by the Internet Architecture Board (IAB) Standard 5.

- IAB Standard 5 is comprised of the IP specification (RFC 791 as amended by RFCs 950, 919, and 922) and integral support protocols
- Internet Control Message Protocol (ICMP), as specified in RFC 792
- Internet Group Multicast Protocol (IGMP), as specified in RFC 1112.

The IP, including ICMP and IGMP, is mandated in the Joint Technical Architecture.

Multicast IP provides the ability to send data to multiple destinations without requiring datagrams to transit any link more than once. It is widely supported by routers and some end systems and should be introduced incrementally. IPv6 is the next generation of Internet Protocol and will be introduced incrementally into the Internet over the next several years. IPv6 incorporates the Multicast IP features as well needed security features. The Naval infrastructure should incrementally evolve toward IPv6 as there are very few products implementing IPv6 and its deployment has been much delayed.

5.3.2.2 Address Resolution Protocol

An address resolution protocol (ARP) is used to determine a data link layer address based upon a specific network layer address. The ARP capability is required for each data link layer supported.

- IAB Standard 36, specified in RFC 1390, defines the transmission of IP and ARP for FDDI networks.
- IAB Standard 37, specified in RFC 826, defines the ARP for Ethernet networks.
- The ARP for ATM is dependent upon the adaptation protocol support capability (i.e., LANE for Ethernet, RFC 1577 for Classical IP over ATM, MPOA).
- RFC 1122, “Requirements for Internet Hosts – Communication Layers”, part of the IAB Standard 3, provides additional guidelines for the ARP.

IAB Standard 37 is mandated in the Joint Technical Architecture.

5.3.2.3 Point-to-Point Protocol

The Point-To-Point Protocol (PPP) provides a protocol independent transport service for datagrams over point-to-point links. Examples of point-to-point links include dial-in from outside the network, router-to-router interconnect, and many satellite lines (by virtue of their engineering). The PPP is Internet Architecture Board (IAB) Standard 51. IAB Standard 51 is specified in RFC 1661 and RFC 1662. Additional guidelines for the PPP are provided in RFC

1122, “Requirements for Internet Hosts --Communication Layers”, part of the IAB Standard 3. The PPP is mandated in the Joint Technical Architecture.

Existing SLIP (Serial Line IP) connections should be incrementally phased out and new SLIP connections should not be supported as PPP is a complete next-generation superset to SLIP and is widely supported by vendors.

5.3.2.4 Obtaining IP Addresses

Official (registered) IP addresses for the U.S. Navy ships and shore commands can be obtained from the Naval Computer and Telecommunications Station (NCTS) Pensacola, Florida at (COMM) 850-452-3501, (DSN) 922-3501. A convenient and efficient method for all ships and unclassified shore commands is the use of the on-line Navy IP Network Number Registration page whose URL is http://www.netreg.navy.mil/. The e-mail address for ships is shipreg@ncts.navy.mil and for shore commands is netreg@ncts.navy.mil. The method for classified shore commands is an on-line Navy IP Network Number Registration page whose URL is http://www.netreg.navy.smil.mil/. The e-mail address is netreg@ncts.navy.smil.mil.

IP addresses are officially tracked and assigned only to the level of a Class C address. The use of subnet masking to subdivide Class C addresses is a matter for local shipboard network administration.

5.3.2.5 Obtaining NSAP Addresses

ATM networks require Network Service Access Point (NSAP) addresses. While the format for NSAP addresses is well defined, the mechanism for obtaining these addresses and properly constructing an ATM topology is still being developed. DISA will administer the DoD NSAP addressing plan and the DON should obtain its addresses from it. NCTS Pensacola is making preparations to provide NSAP addresses to complement IP network address service. The DISA addressing plan is geographically-based for global scalability. It is lacking a robust scheme for deployed forces and mobile users because supporting standards are not yet mature. In the short term, DISA will coordinate with DON users to assign addresses that can be readvertised as deployable forces move. The two options, to be resolved on a case-by-case basis, are to use a geographic address or a reserved globally unique address. In either case, DISA will move the address advertisement within their network as the deployable force moves. When an adequate standards-based mobile protocol exists, DISA will adopt it. A more complete NSAP addressing scheme will be provided in a future version of the ITSG.

5.3.2.6 Use of Proprietary Network Layer Protocols

Proprietary network layer protocols such as Novell’s IPX or Banyan’s Vines IP should not be planned for new systems. However, interoperability between IPX or Vines IP and standard IP will require a network layer gateway and should preferably be avoided.

5.3.3 Transport Layer

This section provides a discussion of the Transport Layer as defined by the OSI Reference Model. The transport layer provides the interface between the network layer protocol and the upper layer protocols. It operates between consenting end systems across the unreliable networking infrastructure to enforce a defined quality of service. The two dominant transport layer protocols used in conjunction with the IP are the Transmission Control Protocol (TCP) and the User

Datagram Protocol (UDP). A third protocol specified but not in use is the Real-time Transport Protocol (RTP).

5.3.3.1 Transmission Control Protocol

The Transmission Control Protocol (TCP) provides a reliable, connection-oriented (end-to-end) transport service used with IP. It supports many application layer protocols such File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) for e-mail and Hypertext Transfer Protocol (HTTP). TCP, while a powerful and ubiquitous protocol, has some limitations that are important to the Naval community. TCP is a unitcast protocol – it does not support multicast. Also, except for error-free transmission (at the application layer), TCP has no precedence or QoS mechanisms. The TCP is Internet Architecture Board (IAB) Standard 7. IAB Standard 7 is specified in RFC 793. Additional guidelines for the TCP are provided in RFC1122, “Requirements for Internet Hosts -- Communication Layers”, part of the IAB Standard 3. Flow control requirements are as specified in RFC 2001. The TCP is mandated in the Joint Technical Architecture.

5.3.3.2 User Datagram Protocol

The User Datagram Protocol (UDP) provides a connectionless, datagram transport service used with the IP. UDP uses whatever quality-of-service is inherent in the underlying structure. For example, if a datagram is lost because of a router overflow, UDP will not detect the loss nor require a retransmission. The UDP is Internet Architecture Board (IAB) Standard 6. IAB Standard 6 is specified in RFC 768. Additional guidelines for the UDP are provided in RFC 1122,”Requirements for Internet Hosts -- Communication Layers”, part of the IAB Standard 3. The UDP is mandated in the Joint Technical Architecture.

5.3.3.3 Real-Time Transport Protocol

The Real-time Transport Protocol (RTP) provides end-to-end transport for applications with real-time characteristics. Examples of such applications include interactive audio and video. The RTP was developed by the IETF and is specified in RFC 1889. RTP usage is not currently widespread.

5.4 Routing and Mobility Protocols

Best Practices

Use Open Shortest Path First version 2 (OSPF 2) for the interior gateway protocol (IGP) and Border Gateway Protocol version 4 (BGP 4) for the exterior gateway protocol (EGP). Use Private Network-to-Network Interface (PNNI) for ATM networks. Use Classless Inter Domain Routing (CIDR) to the maximum extent possible to simplify routing configured -- obtaining IP addresses from NCTS Pensacola with CIDR implementation. Use Dynamic Host Configuration Protocol (DHCP) to provide mobility and conservation of IP addresses.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
IPNetBEUI LAT IGRP RIP DVMRP	OSPF2 for IP IGP BGP4 for IP EGP PNNI for ATM DHCP	OSPF2 for IP IGP BGP4 for IP EGP PNNI for ATM DHCP	OSPF2 for IP IGP BGP4 for IP EGP PNNI for ATM DHCP	OSPF2 for IP IGP BGP4 for IP EGP PNNI for ATM DHCP	MOSPF PIM MBGP
Activities, Platforms, Operational Environments		All. Managed by the ITSC.			

Table 5-6. Network Routing Protocol Recommended Implementations

5.4.1 Routing

Routing protocols are historically defined for IP datagrams, i.e., how does one “route” a datagram from one network (or subnetwork) to another.

Any device is considered a router if it interconnects one or more networks (or subnetworks) and makes forwarding decisions based upon network layer protocol addresses contained in the IP datagrams or ATM call-setup requests it receives. (When only ATM call-setup requests are involved, this function is performed on a switch.) This section specifies a set of routing information and supporting protocols that allows routers and switches to work together and avoids paying certain overhead costs more than once.

The IETF has developed a document which outlines requirements for Internet Protocol (IP) routers, RFC 1812, “Requirements for IP Version 4 Routers.” This document outlines the requirements for support of the IPv4, including support for ICMP, IGMP, ARP, and PPP; as described above. In addition, the RFC provides guidance for routing protocol support and addressing. These standards are consistent with RFC 1812.

The ATM Forum provides standards for the Private Network-to-Network Interface (PNNI) .

5.4.1.1 Addressing

Devices providing the routing function should support both the classical (or hierarchical) IP addressing model and Classless Inter Domain Routing (CIDR). The classical (or hierarchical) interpretation of the Internet address space is that of a 32-bit address partitioned into a network number and a host number; where the network number identifies a hierarchy of addresses and can be further partitioned into subnetworks. CIDR replaces the concept of address classes. The key concepts behind CIDR are:

- The addresses are assigned based upon topology
- Routing protocols are capable of aggregating network layer reachability information
- Use of consistent (longest match) forwarding algorithm.

As part of CIDR, the interpretation of the 32-bit IP address was revised. Instead of fixed-size network and host numbers for the various classes; the address specification refers to a “network

prefix" and a "host prefix." The network prefix is a contiguous string of bits at the most significant portion of the address. The use of the longest match-forwarding algorithm permits more efficient allocation and use of the 32-bit IP address space. CIDR is specified in RFC 1519.

5.4.1.2 Routing Protocols

A routing protocol addresses the need to exchange network reachability information with other routers and end systems. Two basic types of routing protocols are generally used. An interior gateway protocol (IGP) exchanges routing information with other routers, typically within the same administrative domain referred to as an Autonomous System (AS). An exterior gateway protocol (EGP) exchanges routing information with routers that are external to the administrative domain (or between "autonomous systems").

ATM switches exchange routing information using PNNI.

Support for the following routing protocols will provide interoperability with existing and planned systems.

5.4.1.2.1 Routing Information Protocol

The Routing Information Protocol (RIP) is a legacy IGP. Although RIP is identified as IAB Standard 34, it has recently been moved to historical status. The RIP should only be used to support Legacy LAN networks. Support for RIP can be accomplished by the implementation specified in RFC 1058. A second alternative for the support of RIP in legacy systems is the implementation of RIP Version 2 (RIPv2). Although interoperability issues can arise, the RIPv2 specification, RFC 1723, does address interoperability with legacy RIP. RIP should be avoided. (It is included in these discussions because a significant number of equipment manufacturers and users still use this protocol.)

5.4.1.2.2 Open Shortest Path First Version 2

The Open Shortest Path First Version 2 (OSPF2) is also an IGP. It is specified in RFC 1583. RFC 1812, "Requirements for IP Version 4 Routers" recommends the use of OSPF2 for the IGP. OSPF2 is mandated in the Joint Technical Architecture.

5.4.1.2.3 Distance Vector Multicast Routing Protocol

Multicast routing is an evolving technology within the IETF and many vendors are waiting for standards to solidify before providing an implementation. The Distance Vector Multicast Routing Protocol (DVMRP) is the most widely supported of the multicast routing protocols. It was also the basis for much of the Multicast Backbone (MBONE) capability and research efforts involving multicast technology. DVMRP has evolved from its version initial specification (RFC 1075) to its present protocol specification documented in draft-ietf-idmr-dvmrp-v3-04.txt (an Internet Draft). Because it has scaling issues and is not widely supported by vendors, it is not a recommended protocol.

5.4.1.2.4 Border Gateway Protocol Version 4

The Border Gateway Protocol Version 4 (BGP-4) is the EGP recommended in RFC 1812, "Requirements for IP Version 4 Routers". BGP-4 is specified in RFC 1654. BGP-4 is mandated in the Joint Technical Architecture.

5.4.1.2.5 Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a new IETF internal routing standard which is gaining wide support and is therefore in the emerging category.

5.4.1.2.6 Private Network-to-Network Interface

Multicast Border Gateway Protocol (MBGP) is an extension of the exterior routing protocol BGP. It is an emerging standard.

5.4.1.2.7 Private Network-to-Network Interface

There are a number of Private Network-to-Network Interface protocols for ATM (PNNI). All but one, ATM Forum PNNI, is proprietary. A number of manufacturers now offer ATM Forum PNNI. Version 1.0, or Phase 1, is recommended as the preferred standard.

5.4.1.3 Use of Non-Routable Protocols

The use of non-routable protocols such as NetBEUI, LAT, etc., is discouraged. Such protocols do not scale and introduce great difficulties in trying to interconnect multiple networks.

5.4.2 Mobile Addressing

Mobility is currently defined as transportability, i.e., moving a network node from one subnetwork to another but *not* requiring connectivity during the move. This is evolving and will eventually provide for true mobility, i.e., remaining connected during a move. (It is interesting to note that in the wireless area, LEO satellites have the reciprocal effect of mobility, namely, they will be moving so fast (with respect to the user) that the network will move even if the user doesn't. The same protocols can be used in either case.)

5.4.2.1 Dynamic Host Configuration Protocol (DHCP)

DHCP supports several features useful to the Naval network:

- Automatic assignment of IP addresses and configuration data such as netmask and Domain Name System (DNS) server
- Assignment of addresses that are actually used, resulting in economy of IP addresses (unused addresses are reclaimed for reuse)
- Ease of system administration due to automation and ability to administer these details from the server rather than the client.

While DHCP is not intended to support mobile users, it is also valuable in supporting laptop plug in at remote locations. Notably, DHCP actually assigns a new IP address to the end system so the DNS database must change (which requires some settling time) before full service catches up.

5.4.2.2 Mobile IP

Mobile IP is a developing standard within IETF that is designed to support mobile users that move from one domain to another. It operates on a set of home and foreign agents that keep track of forwarding data for a user. In the case of Mobile IP, the end system IP address does not change, so there is no DNS impact.

Mobile IP has considerable value for situations requiring mobile and deploying staffs.

Warning. Both the DHCP and Mobile IP assignment databases contain data that could yield order of battle intelligence so they should be deployed and managed with appropriate attention to security.

5.4.2.3 Mobile NSAP

The need for mobile ATM is just as relevant as for mobile IP. Work is underway to provide an addressing scheme in which one can move their NSAP address as one would move their cellular telephone.

5.5 Quality-of-Service

Best Practices

ATM is the preferred network protocol because of its versatility and its ability to support Quality-of-Service (QoS).

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	ATM	ATM	ATM	ATM	RSVP for TCP/IP
Activities, Platforms, Operational Environments		All. Managed by the ITSC.			

Table 5-7. Quality of Service Recommended Implementations

5.5.1 Description

Quality-of-Service (QoS) is that which provides a level of data transfer which systems can rely on to meet their design goals. For example, if a given application requires a certain minimum bandwidth in which to function properly, it requires that *every* component from the physical media through the operating system guarantee that bandwidth. There are many QoS parameters such as minimum bandwidth, maximum bandwidth, average bandwidth, minimum delay (latency), jitter (delay variation), preemption priority, maximum interrupt time, etc.

At a minimum, the QoS capability of subsystems must be known and bounded so that applications can be designed accordingly. At best, an application will be able to request a particular QoS and receive a high-level of assurance that this “contract” between itself and the lower levels will be honored.

In the network, the first 4 layers of the OSI model must supply QoS. In particular, the bandwidth and delay characteristics of the medium through the processing of data packets and state changes (updating routing information) apply.

QoS is generic in that it affects all communities. DoD is unique in that command and control requires a preemption capability in case of national emergency. DON has additional requirements on board ships and aircraft in that the RF bandwidth to/from these platforms will always be

limited, i.e., one simply cannot supply all the bandwidth a ship/aircraft requires. Managing such limited-bandwidth connections is a challenge.

5.5.2 State

There are three levels of QoS in existence today:

- Best effort
- Provisioned service
- On-demand, negotiated service

5.5.2.1 Best Effort

Best effort QoS is exemplified both by the traditional record message system and by the Internet. As demand exceeds supply, queues form and delays are incurred. As the queues continue to build, a point is reached when the buffers begin to overflow and message traffic is rendered useless due to late delivery or loss. This loss of traffic tends to be non-discriminatory – all users get degraded service.

5.5.2.2 Provisioned Service

Provisioned service is what is used to provide WAN links such as DS-1 and DS-3. The customer requests a dedicated circuit at a particular rate between two points. This circuit is established and is guaranteed to be “up” and under full control of the user. While this is guaranteed, it can become prohibitively expensive. For example, if a user needs an OC-3 peak (155 Mbps) for only short periods throughout the day, one must pay for the entire circuit 24 hours per day.

5.5.2.3 On-Demand, Negotiated Service

On-demand, negotiated service is analogous to the telephone system. Once places a call on demand. If the call goes through, the user is happy. If, however, it is blocked (a busy signal), the user is not happy. Also, an existing call may be dropped if a higher-priority call comes through (FLASH, for example). In modern networks there are more than two levels (call gets through or doesn’t). Usually virtual circuits are established but IP datagrams or ATM cells are individually delayed, or even blocked. Most applications will retransmit and the user simply sees a momentary delay.

5.5.2.4 Summary

All models are of value in the military. Under best effort, if the occurrence of delay is visible to users, it becomes a feedback mechanism that assumes that users will discipline themselves to restrict traffic to that essential to business. This model tends to be fairly resilient, albeit frustrating, under stress.

The provision service provides the guaranteed QoS that critical command and control systems need. For example, data may have completely lost its value if it arrives too late. The class of service, however, is expensive and cannot respond quickly to changing requirements.

The on-demand, negotiated model is very important in that it can respond quickly to changes in requirements.

QoS features in various network protocols are designed to meet various facets of one of these models. But the problem is complex – it pervades every layer of the ISO Reference Model. For example, it is of no use to have the network provide a guaranteed minimum delay if the operating system cannot also honor this "contract." Also, other factors greatly affect the network's ability to provide a given level of QoS. For example, the amount of interleaving in forward error correction (physical), packet size and media access method (data link), router and switch configuration (network) and transport protocol error correction doctrine (transport) are all pertinent examples.

The various recommended protocols in this chapter address different aspects of the QoS problem:

- Homogenous ATM networks (LANs or WANs) can offer QoS guarantees to the workstation.
- Standards work in the ATM Forum is proceeding to allow applications to specify QoS parameters to the network.
- Within single segment LANs, FDDI offers deterministic service. Ethernet provides a best-effort service. Neither can offer QoS guarantees across a WAN.
- Standards work in the IETF is proceeding to offer both preferential non-deterministic service and bounded delay service upon implementation of RSVP (Resource Reservation Protocol). In order to operate to scale, all routers between end systems must be RSVP-capable and the end systems must be RSVP-protocol aware in order to request resources from the routers.

The mechanisms to control quality of service in the network in its larger dimension (more than one segment) are still maturing. Further, the doctrine and management structure to control the mechanisms when they are available is evolving. Nonetheless, we should be looking to incorporate tools, as they become available.

5.6 References

5.6.1 Standards and Specifications Resources

Physical and Data Link for the LAN

Naval Sea Systems Command (NAVSEA) document: "NIIN IPT Near term Guidance for Shipboard Networks", 11 November 1997

Institute of Electrical and Electronics Engineers (IEEE) standard; IEEE 802.1d, Spanning Tree for Network Reconfiguration

Laubach (Hewlett Packard); ,"Classical IP over ATM" (RFC 1577); January 1994; ftp://ftp.isi.edu/in-notes/rfc1577.txt (23 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard; IEEE 802.1Q, "Draft Standard for Virtual Bridged Local Area Networks"

Institute of Electrical and Electronics Engineers (IEEE) standard; IEEE 802.10 "Link-layer Standard for Interoperable LAN Security (SILS)"

Institute of Electrical and Electronics Engineers (IEEE) specification; IEEE 802.11-1997 "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY)"

Institute of Electrical and Electronics Engineers (IEEE) standard; IEEE 801.1p, Standard for Local and Metropolitan Area Networks – Supplement to Media Access Control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering

ATM Forum specification, af-uni-0010.002: "ATM User-Network Interface Specification V3.1, 155.52 Mbps Optical Interface", 1994, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-phy-0046.000 662.08 Mbps Optical Interface, January 1996; www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-phy-0054.000 44.736 Mbps Coax Interface, March 1996, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

Physical and Data Line Protocols for Radio Communications

Department of Defense (DOD) MIL-STD-188-181A, Interoperability Standard for Single Access 5 kHz and 25 kHz UHF Satellite Communications Channels, 31 March 1997

Department of Defense (DOD) MIL-STD-188-182A, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 31 March 1997

Department of Defense (DOD) MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, dated 2 December 1996

Department of Defense (DOD) MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993

Department of Defense (DOD) MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995.

Department of Defense (DOD) MIL-STD-188-166 (Interface Standard, Interoperability and Performance of Non-Electronic Protective Measures (EPM) for SHF SATCOM Link Control Protocols and Messaging Standards)

Department of Defense (DOD) MIL-STD-188-167 (Interface Standard, Message Format for SHF SATCOM Demand Assignment)

Department of Defense (DOD) MIL-STD-188-168 (Interface Standard, Interoperability and Performance Standards for SHF Satellite Communications Multiplexors and Demultiplexers)

Department of Defense (DOD) MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995

Department of Defense (DOD) MIL-STD-1582D, EHF LDR Unlinks and Downlinks, September 30, 1996; with Notice of Change 1, dated 14 February 1997

Department of Defense (DOD) MIL-STD-188-136, EHF MDR Unlinks and Downlinks, August 26, 1995; with Notice of Change 1, dated August 15, 1996, and Notice of Change 2, dated 14 February 1997 Katz (Cisco); “Transmission of IP and ARP over FDDI Networks” (IAB Standard 36/RFC 1390), January 1993; ftp://ftp.isi.edu/in-notes/rfc1390.txt (23 May 1998)

Department of Defense (DOD) MIL-STD-188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard, September 15, 1988; with Notice of Change 1, dated 17 June 1992, and Notice of Change 2, dated 10 September 1993

Department of Defense (DOD) MIL-STD-188-148A, Interoperability Standard for Anti-Jam Communications in the HF Band (2-30 MHz), 18 March 1992

Department of Defense (DOD) MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985

Department of Defense (DOD) MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, 15 March 1989

Department of Defense (DOD) MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 7 May 1987; with Notice of Change 1, 28 July 1992

North American Treaty Organization (NATO) standard: STANAG 4246, “HAVE Quick UHF Secure and Jam-resistant Communications Equipment”, Edition 2, 17 June 1987; with Amendment 3, August 1991, /www-library.itsi.disa.mil/org/stanag/4246.htm (23 May 1998)

Space and Naval Warfare Systems Center (SPAWAR) Joint Maritime Communications System (JMCOMS) web page: www.jmcoms.org (23 May 1998)

Teledesic Corporation web page: www.teledesic.com (23 May 1998)

Inmarsat web site: www.inmarsat.org (23 May 1998)

Internet Protocols

Postal (USC ISI); “Internet Protocol” (RFC 791), September 1981, http://info.internet.isi.edu:80/in-notes/rfc/files/rfc791.txt (23 May 1998)

Postal (USC ISI); “Internet Control Message Protocol (ICMP)” (RFC 792); September 1981; ftp://ftp.isi.edu/in-notes/rfc792.txt (23 May 1998)

Postel (USC ISI); “Transmission Control Protocol” (RFC 793/IAB Standard 7) September 1981; ftp://ftp.isi.edu/in-notes/rfc793.txt (23 May 1998)

Plummer (MIT) “An Ethernet Address Resolution Protocol” (IAB Standard 37/RFC 826) November 1982; ftp://ftp.isi.edu/in-notes/rfc826.txt (28 May 1998)

Mogul (Stanford) “Broadcasting Internet Datagrams in the Presence of SubNets” (RFC 922), October 1984; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc922.txt (23 May 1998)

Mogul (Stanford), Postal (USC ISI); “Internet Standard Subnetting Procedure” (RFC 950), August 1985; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc950.txt (23 May 1998)

Mogul (Stanford); “Broadcasting Internet Datagrams” (RFC 919); October 1984; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc919.txt (23 May 1998)

Waitzmen, Partridge (BBN), Deering (Stanford); “Distance Vector Multicast Routing Protocol” (RFC 1075); November 1988; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1075.txt (23 May 1998)

Deering (Stanford); “Internet Group Multicast Protocol (IGMP)” (RFC 1112) August 1989; ftp://ftp.isi.edu/in-notes/rfc1112.txt (23 May 1998)

Braden (IETF); “Requirements for Internet Hosts – Communication Layers” (RFC 1122), October 1989; ftp://ftp.isi.edu/in-notes/rfc1122.txt (23 May 1998) (part of the IAB Standard 3, provides additional guidelines for the ARP)

Katz (Cisco); “Transmission of IP and ARP over FDDI Networks (RFC 1390/IAB Standard 36); January 1993; ftp://ftp.isi.edu/in-notes/rfc1390.txt (23 May 1998)

Fuller (BARRNet), Li (Cisco), Yu (MERIT), Varadhan (OARNet); “Classless InterDomain Routing (CIDR)” (RFC 1519), September 1993, http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1519.txt (23 May 1998)

Moy (Proteon); “Open Shortest Path First Version 2” (RFC 1583), March 1994; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1583.txt (23 May 1998)

Simpson (Daydreamer); “The Point-to-Point Protocol (PPP)” (RFC 1661/Standard 51); July 1994; ftp://ftp.isi.edu/in-notes/rfc1661.txt (23 May 1998)

Simpson (Daydreamer): “PPP in HDLC-like Framing” (RFC 1662/Standard 51); July 1994; ftp://ftp.isi.edu/in-notes/rfc1662.txt (23 May 1998)

Baker (Cisco); “Requirements for IP Version 4 Routers” (RFC 1812), June 1995; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1812.txt (23 May 1998)

Postel (IAB) “Internet Official Protocol Standards” (RFC 1880/IAB Standard 1); November 1995; ftp://ftp.isi.edu/in-notes/rfc1880.txt (23 May 1998)

Schulzrinne (GMD Fokus); “Real Time Transport Protocol (RTP) Profile for Audio and Video Conferences with Minimal Control” (RFC 1890); January 1996; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1890.txt (23 May 1998)

ATM Protocols

ATM Forum specification, af-uni-0010.002 User-Network Interface (UNI) 3.1, 1994, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-sig-0061.000 User-Network Interface (UNI) Signaling v4.0, July 1996, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-sig-0076.000 User-Network Interface (UNI) Signaling Addendum, January 1997, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-pnni-0055.000 Private Network-to-Network Interface (PNNI) 1.0 (Phase 1), March 1996, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-pnni-0026.000 Interim Inter-switch Signaling Protocol (IISP) (PNNI Phase 0), December 1994, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-lane-0021 LAN Emulation (LANE) 1.0, January 1995, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-mpoa-0087.000 Multiple Protocol Over ATM (MPOA) 1.0, July 1997, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

Obtaining IP Addresses:

For IP Addresses and support, the URL is http://www.netreg.navy.mil/. The e-mail address is shipreg@ncts.navy.mil, for ships and netreg@ncts.navy.mil for shore. Classified shore commands should use http://www.netreg.navy.smil.mil/ for the URL and netreg@ncts.navy.smil.mil for e-mail.

Obtaining NSAP Addresses:

Use the same address provided above in “Obtaining IP Addresses”. The DISA ATM Addressing plan is available on the World Wide Web at URL http://www.disa.atd.net/DISNATM_DOCS/.

5.6.2 Supporting Resources

Breyer and Riley, Switched and Fast Ethernet: How it Works and How to Use It, Ziff-Davis Press, Emeryvile, CA; 1995

Bryce, Using ISDN, Second Edition, Que Corporation, Indianapolis, IN, 1996

Hines, ATM, The Keys to high-Speed Broadband Networking, M&T Books, New York, NY; 1996

6. Information Distribution

This chapter includes core network applications common to all users including electronic mail, web services, file transfer, and directory services. The relationship of this chapter with the ITSG is shown in Figure 6-1.

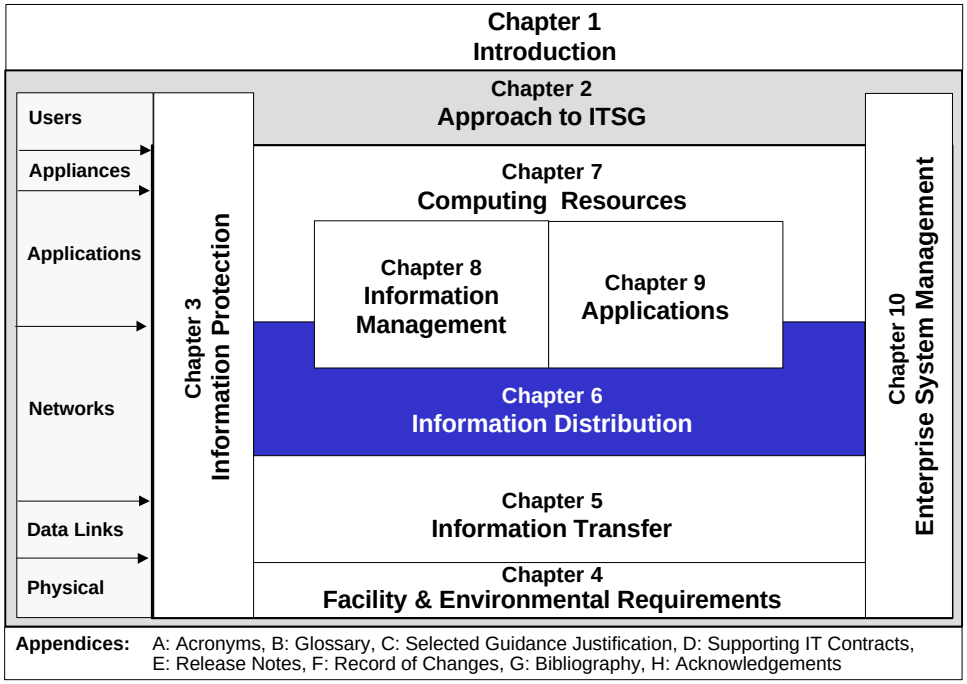


Figure 6-1. ITSG Document Map Highlighting Chapter 6, Information Distribution

6.1 Overview

Information distribution is effectively the "nerve center" of the information technology paradigm. As shown in Figure 6-1, information distribution is the nexus of information protection, information transfer, computing resources, information management, applications and enterprise system management. It is the zone where communication technologies meet computer processing technologies. Where in the past both of these technologies had their separate cultures, information distribution brings these two cultures together enabling a new, more comprehensive and effective information technology culture.

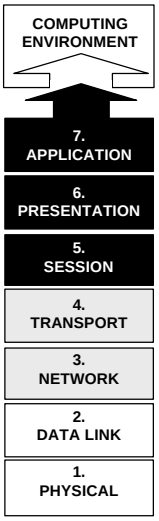


Figure 6-2. ISO/OSI Model Layers 5 - 7+

Whereas Chapter 5, Information Transfer, focused on the first four layers of the International Standards Organization/Open Systems Interconnect (ISO/OSI) seven layer model, Chapter 6, Information Distribution, extends the Transport and Network layer and completes the last three layers, Session, Presentation, and Application, into the computing environment (Figure 6-2).

The term "information distribution" is short for a more descriptive term: Basic Network and Information Distribution Services (BNIDS). BNIDS organizes the network and provides fundamental applications that all users in all functional

areas require. BNIDS includes the configuration of the network and network devices to establish node, user and device identification, system domain establishment, a routing or switching schema to move information to its final destination, security services, directory services, electronic mail (e-mail) including attachments, electronic dialog (chat), and web services (http). Figure 6-3 summarizes BNIDS by using the standard ITSG method of placing the foundation technologies on the bottom and working toward the user at the top.

As shown in Figure 6-3 Figure 6-3, there are 13 items that will be described in order. The concept of operations provides the context in which all BNIDS technologies fit together to give the user an integrated product.

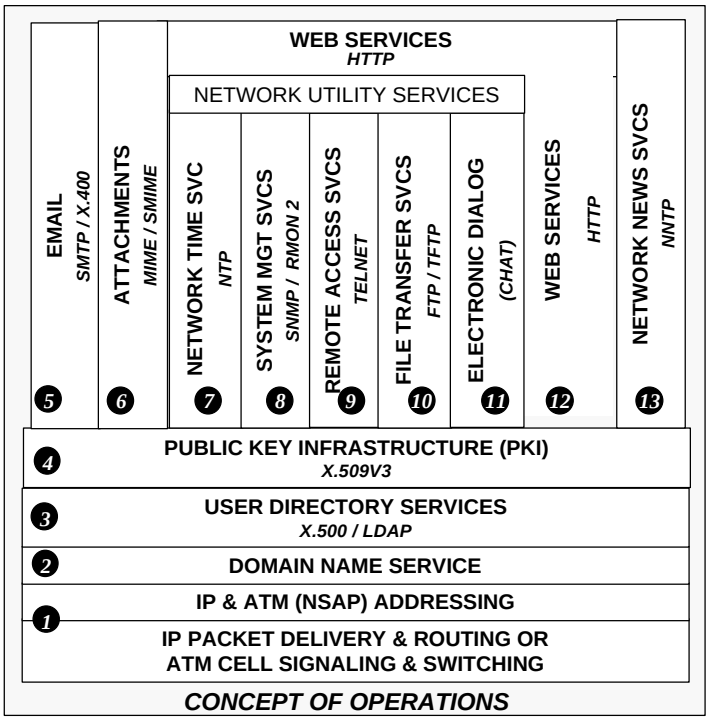


Figure 6-3. Basic Network and Information Distribution Services (BNIDS) Showing the Order of Discussion

The five technologies at the bottom are pervasive to all of the BNIDS and support the upper level technologies.

IP Packet, Delivery, IP Addresses, ATM Cell Delivery and NSAP Addresses are all information transfer technologies covered in Chapter 5.

Domain Name Service (DNS) allows people to specify network device addresses in more friendly (human readable) terms.

User Directory Service allows any system or user of the information infrastructure to find the electronic office or mail home of another person or organizational entity.

Public Key Infrastructure supports protection of information content during transfer across the network thereby supporting need-to-know among trusted users. It also provides a trusted login server to support greater accessibility with adequate protection.[5]

The nine technologies shown in Figure 6-3 as vertical columns are specific to particular functions that are common to all users and system devices.

Electronic Mail (e-mail) permits transfer of messages between users, organizational entities, and groups of users.

Attachments allow attaching files in any media to an e-mail message. These attachments can be documents, programs, sound bites, animations, video clips, entire videos, etc.

Network Time Service permits synchronization of clock time among the many system devices that have to interact across the network. Each device has minute variations in clock speed that accumulate over time and can potentially affect operations (e.g., a "future time late" because of a time-stamp from a source clock that is faster than a destination clock).

System Management Services goes beyond remote access in that it provides a set of standard protocols that allow monitoring, collection of data and control of the system devices.

Remote Access Services support logging into remote computers and network devices from distant management centers to primarily perform administrative tasks. This feature supports centralized management of distributed devices but inherits a significant security risk that must be mitigated through other means.

File Transfer Service permits the direct push or pull of information files (any media) from one computer to another.

Electronic Dialog allows real-time (or near-real-time) conversations to occur over the network. Normally this service is associated with teletype 'chat' which uses relatively low bandwidth and is useful for troubleshooting over links with small data rates. It does not include voice, telephone and video teleconferencing services because these services demand relatively high bandwidth and are not available to all users (tactical and non-tactical).

Web Services allow users to traverse the network to various information sources through a network ("web") of objects (words, pictures, icons, etc.) linked to other files and information sources.

Network News Services allow creation and sustainment of electronic, interactive bulletin boards to support a running dialog or notice of current events, status, direction or debate.

The standards and guidance associated with Figure 6-3 and the preceding summary of BNIDS will be expanded through the rest of this chapter. First, a BNIDS concept of operations is described, followed by amplifying sections on domain name services, directory service, public key infrastructure, e-mail and attachments, network utilities, and web services. The e-mail section

[5] A complete description of Public Key Infrastructure (PKI) is provided in Chapter 3, Information Protection. Accessibility is a metric discussed in Chapter 10, Enterprise Management.

includes a detailed DON implementation strategy. The web services section provides valuable guidance on this rapidly emerging technology.

6.2 Concept of Operations for BNIDS

Command, Control, Communication, Computers, and Intelligence (C4I) for the Warrior, Copernicus, Information Technology for the 21st Century (IT21), and Marine Air Ground Task Force (MAGTF) C4I are similar system integration strategies that focus on tailoring the information infrastructure to support the common user. For BNIDS, the user is the warfighter, operator, marine or sailor. The user is the focus of the concept of operations.

6.2.1 Official Individual Accounts

Figure 6-4 depicts the user-centric focus on the officer, enlisted, and civilian as the critical component of all DON organizational structures. As discussed in Chapter 2, the DON is a very dynamic environment because of individual assignment rotations, embarking commands, and force movements. For Navy and Marine Corps, this environment renders as unsuitable many of the structures and protocols directed at the commercial world.

Official individual e-mail accounts help to address this dynamic situation. To enhance mission effectiveness, every individual in the DON will have an official account with an associated e-mail address. The individual will maintain his or her information system identity wherever they go during their Naval career. Individuals will be allowed to choose their own official e-mail address within some liberal formatting constraints. The individual e-mail address will be less than twelve characters in length. Nicknames, call signs, last names, first names will all be acceptable so that individuals gain a sense of ownership of their information system identities. The e-mail address can be put on business cards without requiring a change of cards upon command reassignment. Official individual business, such as detailing, fitness reports, and promotions can be conducted using the official individual account. The official individual account will always be on the unclassified part of the infrastructure, and changing an individual address will be allowed but not encouraged.

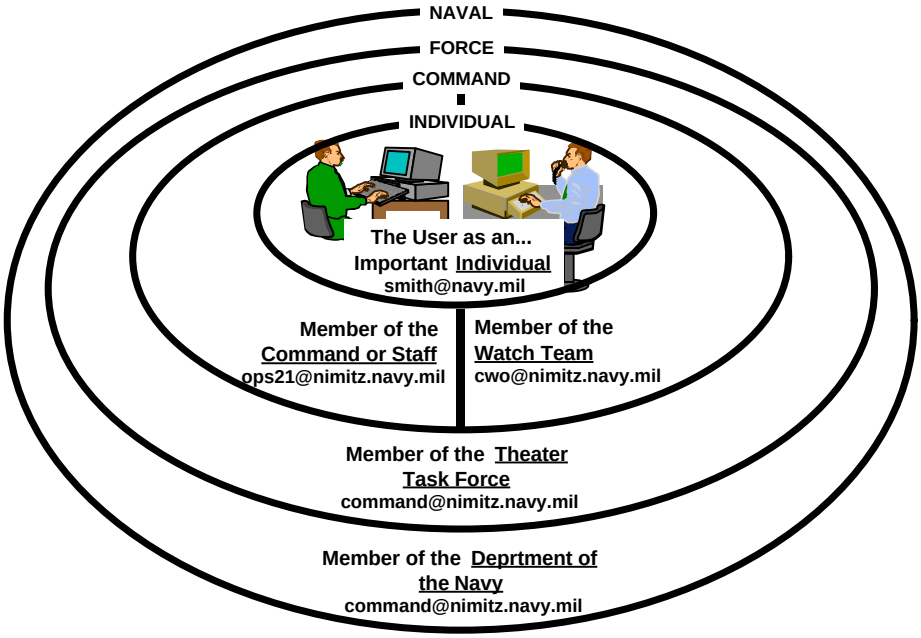


Figure 6-4. User-Centric View

Because it will be assigned to the Navy or Marine Corps system domain, the user's official individual account will move with the individual to a new assignment but remain unchanged. For example, a marine and a sailor are shown in Figure 6-4. The marine's name is GSGT Jones and the sailor's name is Petty Officer Smith. Jones has selected "jones" for his e-mail address and Smith selected "smith". Jones' full Simple Mail Transfer Protocol (SMTP)[6] e-mail address would be "jones@usmc.mil" and Smith's would be "smith@navy.mil"[7]. Each individual's official office account will reside on his/her command's file server either at the command itself or at the servicing Information Technology Service Center (ITSC)[8]. Upon transfer, the individual's official account will be transferred to the ITSC closest to the individual's next command where he or she will continue to receive e-mail and conduct official business (including family correspondence). The ITSCs will provide a 90 day transfer account to allow a graceful transition from the old to the new command. Again, the concept calls for Smith, Jones and all DON members to keep their official individual account throughout their career, wherever they are, even during transfer periods.

6.2.2 Command/Staff Accounts

As a member of the command or staff, each individual must also maintain an identity associated with the organization. For this, individuals would also have staff or command accounts with an identity associated with the command position or staff code. Unlike the official individual account, the command or staff account is rigidly formatted so that the command identity remains consistent, independent of the individual that holds the position. The individual may have as many as three command/staff accounts corresponding to the Unclassified, Secret and potentially

[6] SMTP was chosen because of its pervasiveness on DISN and the Internet and that it is presently more portable than X.400. This is described in the e-mail standards guidance provided in Section 6.5.

[7] The Information Technology Service Center would ensure that their names are unique within their domain.

[8] See Chapter 10 for a full description of the Information Technology Service Center (ITSC) concept.

Sensitive Compartmented Information (SCI) classification systems. To support this concept, each command and staff must establish staff codes or command positions to have an identity on the information infrastructure. (For example, "MPA" for Main Propulsion Assistant would have an account name and e-mail address of MPA@shipname.navy.mil.)[9]. Users can have their official individual e-mail forwarded to their command/staff account by the ITSC. This will be allowed and encouraged. Users could have their command/staff e-mail forwarded to their official individual account if there is a rational requirement, but generally, this practice will be discouraged.

6.2.3 Duty/Watch Accounts

Another command/staff virtual identity that must be represented in the information infrastructure is the duty or watch team. Members of the duty or watch team rotate daily but the command identity remains constant and is often the most critical position of the staff or command. As individuals assume the staff position they also assume ownership and all attendant responsibilities associated with the watch account. This watch identity is shown on Figure 6-4 in the right side of the command circle. Forwarding of official individual e-mail or command/staff mail will not be permitted.

6.2.4 Command Correspondence and Distribution Lists

Until Defense Message System (DMS) becomes fully operational, the following concept can be used to conduct command correspondence using SMTP. For command correspondence, each command will have an e-mail address of "command@command_name.navy.mil" for unclassified e-mail and "command@command_name.navy.smil.mil" for classified e-mail. "Command" in this case is a special account where e-mail from "command@command_name.navy.mil would have official command intent, direction, or information dissemination as provided by the Commanding Officer or his designated representative with command correspondence release authority. The Commanding Officer would still have a command/staff account (co@command_name.navy.mil) as well as his official individual account for his command and individual e-mail (e.g., co's_lastname@navy.mil). E-mail delivered to "command@command_name.navy.mil" will be forwarded to an internal distribution list determined by the commanding officer or chief of staff. An anticipated distribution for "command@command_name.navy.mil" could be the duty officer, the executive officer, and a message profiler application that will forward the mail based upon key words in the text of the message itself. The use of a distribution list for expeditious delivery of command correspondence is extremely valuable. Other distribution lists could be used for special circumstances such as cat@command_name.navy.mil for a Crisis Action Team (CAT), or ato@command_name.navy.smil.mil for Air Tasking Order (ATO) planning. Members of the command, assisted by the ITSC, would manage these distribution lists. Mixing user names and command names on command correspondence e-mail is permitted. As in JANAP 128 record messages, the "To" line to designate "action required" versus the "Cc" line for "information purposes" should be maintained. Proper process dictates that the command/staff accounts should be receive-only, to ensure that originators of messages can be properly identified.

[9] Examples used in this section use the Navy's domain for consistency. For all "navy.mil" examples, "usmc.mil" could be substituted for the same intent.

6.2.5 Directory Services

An enterprise directory service is required to track official individual accounts, command/staff accounts, duty/watch accounts, and distribution lists. This task would be challenging enough if the managed entities were not in a constant state of flux, as they are in the Navy and Marine Corps. The server that the user accesses to retrieve and send mail, as well as to conduct normal office automation tasks is referred to as his home account. (The home account can be referred to as a user's "mail home".) The home account moves at the discretion of the command or the user in the case of transfer or long term temporary duty. Commands or command elements that embark or deploy take their home accounts with them. Official individual home accounts would likely not move during embarkations or deployments but command/staff, watch accounts, and distribution lists would move.

Tracking and promulgating the location of the home account-e-mail address pairs would be the responsibility of X.500 *master directories* maintained by both the Navy and the Marine Corps to service each classification level (Secret Internet Protocol Routing Network (SIPRNET) and Non-classified Internet Protocol Routing Network (NIPRNET)). These master directories would be maintained at a central location with at least one backup at an alternate location. The master directory would likely be maintained by an ITSC which would serve as an X.500 source directory. There would be X.500 replication directories at each fleet teleport, and alternate locations determined by the Marine Corps, and in the San Diego region for performance and reliability. The Navy and Marine Corps X.500 directories would be linked with the Coast Guard's X.500 directory for full maritime coverage. Home account servers will employ the Lightweight Directory Access Protocol (LDAP) to access the X.500 source or replication directories to carry as much of the full X.500 directory as they need to perform their mission (Figure 6-5). Ships and tactical commands with limited communication bandwidth need to update their e-mail directories while in port or in garrison prior to getting underway or deploying.

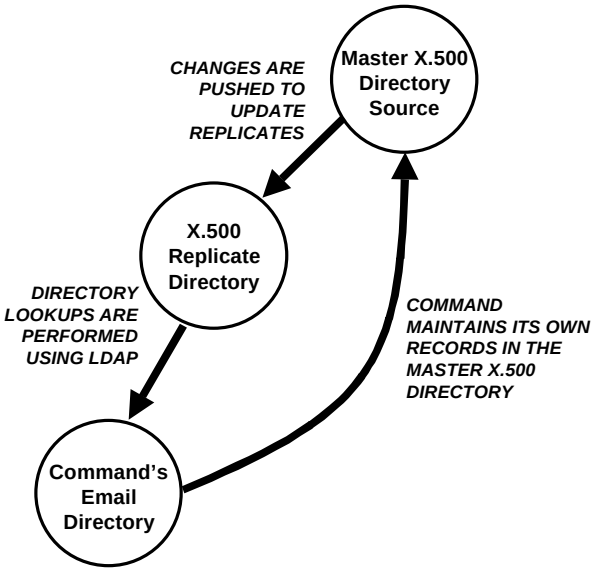


Figure 6-5. X.500 Directory Update and Maintenance

The Command Information Officer (CIO) should be established as the member of the command to coordinate with the ITSC to update the Navy or Marine Corps Master X.500 Directory (MXD).

Either the Command's CIO or the user will be able to update his own official individual record. Only the Command's CIO (or the Commanding Officer's designated officer) will be able to update command/staff accounts and command distribution lists. In all cases, commands will be responsible for maintaining their records in the Master X.500 Directory.

6.2.6 Defense Message System (DMS) Interoperability

DMS will become the official message delivery system in the DoD. The concept for DMS is to replace the aging Automatic Digital Network (AUTODIN) with an open standards-based system comprised of commercial products. DMS is based upon the X.400 e-mail standard and X.500 directory standard with special military alterations to meet the Required Operational Message Capability (ROMC). The DMS concept calls for the replacement of command-to-command formatted messages with writer-to-reader messages and multi-media attachments. Each individual message delivery would be protected through encryption and decryption of each message using Fortezza PC cards at the user's personal workstation. Messages would be either individual traffic (analogous to personal e-mail) or organizational traffic (analogous to the command correspondence concept described in Section 6.2.4 above).

Figure 6-6 illustrates this concept. A parallel design should also be used to support the SCI DMS requirements. As shown there are two DON DMS users, one on each fleet; there are two Navy SMTP-only commands, one on each fleet; and there is a cloud representing the community of DMS users in the DOD as well as a cloud representing the SMTP users in DoD. Seven cases of e-mail delivery are shown. All Navy and Marine Corps DMS traffic flows through one or more of the three MFI mail switches. DMS traffic flowing internal to the DON can use X.400 or a protocol employed by the mail switches and associated User Agents installed at the DMS user site's DMS server suite. DMS messages delivered outside of the DON will be translated to DMS-standard X.400 for subsequent delivery. The MFI mail switch will also receive DMS X.400 messages and commercial X.400 messages and translate them to SMTP for further delivery to any Naval command. All Naval commands, DMS or not will use SMTP to ensure tactical and tactical-support communication. Table 6-1 summarizes the DON interoperability with DMS.

To interface elements of the DON's dynamic environment that require SMTP e-mail with DMS that requires X.400 (e.g., for tactical and tactical support implementations), at least three sets of mail switches should be employed to serve as DMS Multi-Function Interpreters (MFIs). A set of mail switches will involve a pair of mail switches, one on the NIPRNET and one on the SIPRNET to maintain a consistent architecture on both the Secret and Unclassified networks. The three mail switch sets should be distributed as follows: one for the Marine Corps, one for the Atlantic Fleet and one for the Pacific Fleet. These MFI mail switches will support delivery of DMS traffic within the DON as well as to other DOD organizations.

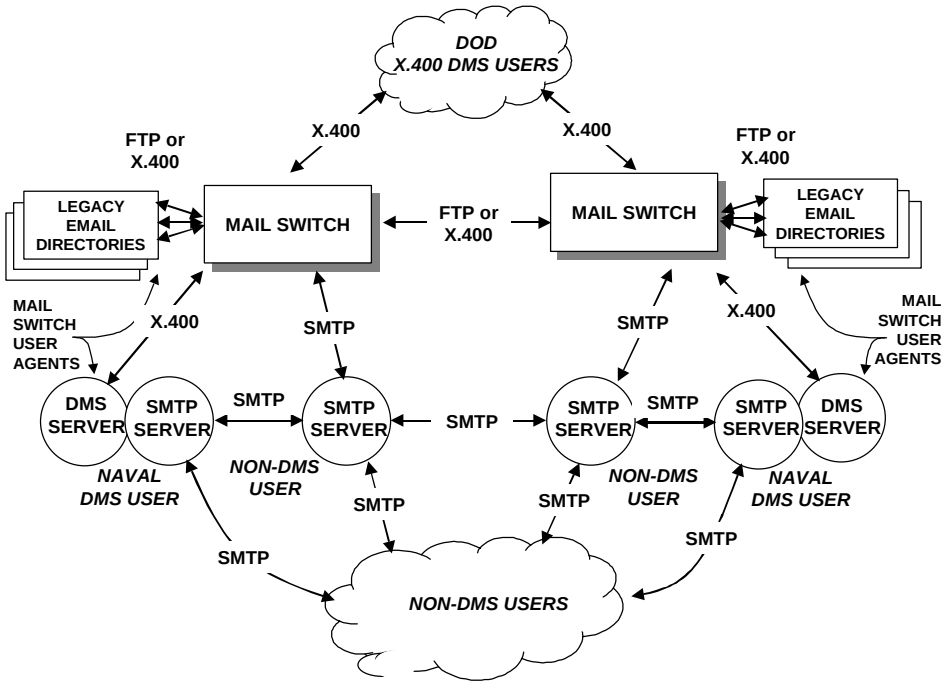


Figure 6-6. DMS Multi-Function Interpreters

		Path Description	
From	**To**	**Link**	**Protocol**
Navy DMS Site	SMTP Site	Navy DMS to MS MS to SMTP Site	X.400 SMTP
SMTP Site	Navy DMS Site	NA	Not Applicable. DMS only receives from authorized DMS sites.
Navy DMS Site	Navy DMS Site	Navy DMS to MS MS to MS MS TO Navy DMS	X.400 X.400 X.400
Navy DMS Site	DOD DMS Site	Navy DMS to MS MS to DOD DMS	X.400 X.400
DOD DMS Site	Navy DMS Site	DOD DMS to MS MS to Navy DMS	X.400 X.400
DOD DMS Site	Navy SMTP Site	DOD DMS to MS MS to Navy SMTP	X.400 SMTP
Navy SMTP Site	DOD DMS Site	NA	Not Applicable. DMS only receives from authorized DMS sites.
SMTP Site	SMTP Site	No gateways or interpreters	SMTP

Note: For above, MS means Mail Switch

Table 6-1. Interim DMS Interoperability with the DON Information Infrastructure

6.2.6.1 Directory Synchronization Side Benefit of the DMS MFI

A side benefit of the mail switch is that some products also translate native legacy e-mail directories into standard X.500. This feature should be acquired and used to maximize e-mail interoperability to all e-mail users as an interim measure until they can employ a X.500/LDAP based e-mail system. The mail switch could be used as a backup to the Master X.500 Directories. As changes occur through time, various e-mail directories will become outdated if subsequent updates are not made to the Master X.500 Directory. To minimize this effect, mail switch's directory synchronization capability can be used to automatically update outdated directory information. This occurs as commands with ownership of accounts change their directories; the mail switch will automatically detect and promulgate the changes to other participating e-mail servers.

6.2.7 Security Certificate and Login Services

To support information content and need-to-know protection, X.509v3 digital security certificates will be used to provide secure web connections (through Secure Socket Layer (SSL)) and encrypted e-mail attachments (through Secure Multipurpose Internet Mail Extension (S/MIME)). A complete description of the Public Key Infrastructure (PKI) used to support Security Certificate and Login Services is provided in Section 3.5. PKI could support a common login server that would manage secure connections to the multitude of applications, information bases and servers that a user must traverse to collect required information in a network centric world. Rather than remembering a unique account and password for every server or application encountered, servers and applications would maintain a trusted relationship with the login server who would provide the necessary security parameters while the user collects the required information. At this time, establishing a common login server is too risky to pursue at the DON enterprise level but additional security using SSL and S/MIME is very beneficial. Security certificate authorities should be established and managed across the DON to appropriately support both fleet and shore based activities The certificates and certificate revocation lists should be stored in the Master X.500 Directories. The official DON policy for implementation of PKI is provided in Section 3.5.

6.2.8 Web Drop and Pickup Service

Web Drop and Pickup (WDP) service offers an alternative method to e-mail attachments to transfer large files (e.g., greater than 2 MB). A WDP Server must be established either at a servicing ITSC or at one of the commands involved in the file transfer. The sender of the large file uploads the file to the WDP Server then sends an e-mail message to the intended recipients with the hyperlink or instructions on how to fetch and download the file. This service improves information management efficiency by allowing the recipient to download the large file at his convenience and when he has the bandwidth to do so (e.g., on the road with a slow speed modem). Additionally, the file does not consume the recipient's internal disk space if he decides that he does not need it. The network is less burdened by "pushed" attachments that are not necessarily needed. The sender is comforted to know that his attachment was less likely to cause an unintentional "denial-of-service" on his recipients through clogging their e-mail channel.

6.2.9 BNIDS CONOPS Summary

A concept has been presented that supports the following operational requirements:

- Official Individual Accounts And E-mail Addresses Held During An Individual's Entire Career
- Command/Staff User Accounts and E-mail Addresses
- Watch Accounts and E-mail Addresses
- Home Accounts/Mail Homes
- Command Correspondence
- Command Distribution Lists
- Individual Transfer Between Duty Stations
- Embarkation And Disembarkation of Highly Mobile Commands
- Directory Services Including Downloads, Updates, and Maintenance
- Interoperability With DMS
- Directory Synchronization
- Digital Security Certificates for Secure E-mail Attachments and Secure Web Links
- Web Drop and Pickup Service

This concept provides the context in which standards and guidance is provided for each of the BNIDS technologies to follow.

6.3 Domain Name and Directory Services

Naming and directory services are needed to locate resources on the network. These services provide the means for identifying and retrieving information about objects on the network. An object is a specific resource on the network such as a computer, application, file, e-mail box, printer, or router. Information that can be retrieved about an object varies according to the object and the name or directory service providing the information.

Naming and directory services are related in the functions they provide, but distinct differences exist. A naming service locates and retrieves information about an object solely by the name of the object. There are stand-alone systems, such as Internet Domain Name Service (DNS), that implement a naming service. However, most are integrated within other services, such as file systems and e-mail. Examples of integrated naming services are the name and address books within Lotus Notes, MS Exchange, and NetWare's file services.

In a directory service, each object is identified and retrieved based on its attributes, where one of the attributes is its name. This service provides the additional capability of searching for all objects that have one or more particular attributes — for example, "What are the names of all DON employees located in Crystal City?"

A new method of combining multiple directories, called meta-directories, is evolving. Meta-directories provide application-specific agents that synchronize the application directories (e-mail and operating systems) into a standard directory with access via the Lightweight Directory Access Protocol (LDAP).

6.3.1 Domain Name Service (DNS)

DNS translates computer host and network device IP addresses into understandable names and visa versa. It uses TCP/UDP as a transport service when used in conjunction with other services. The DON domains for NIPRNET are navy.mil and usmc.mil; for the SIPRNET it is navy.smil.mil and usmc.smil.mil.

A consistent, globally unique naming and addressing scheme is the key element in successfully implementing client/server applications and environments. This naming scheme is required for the objects being stored in directory systems. The names of the objects need to be logical and meaningful to the system users and to other applications. A name needs to conform to four specific principles:

- Alphanumeric, clearly conveying the built-in meaning
- Unique within its domain
- Not overly encoded or hexadecimal, except for security purposes
- Names and addresses of network entities must be globally unique to construct enterprise networks

Best Practices

Domain names for commands should be short but understandable abbreviations of the command name. The primary domain name for ships is the type and hull number with no dash, space or

punctuation in between. The ship name shall also be available as a domain name as an alias. Ships named after people should use only the last name for brevity. Where two ships are named after a distinguished individual with the same last name, at least one of the domain names should have the initial of the first name or enough of the first or middle name to attain a unique domain name. Use of commonly understood initials of the dedicated individual is also acceptable as a domain name of the ship (e.g., JFK, FDR). Shore commands shall use an abbreviation of their administrative name as the primary domain name rather than the task force designation. Commands with a permanent task force designation can have an alias domain name with the task force designation. Domain names for command attachments shall use the standard command domain name with the detachment designation directly appended with no space, underscore or dash.

The Network Information Center (NIC) requires that all DNS Servers have at least one secondary DNS at a remote location. For ships the primary DNS will be ashore at its servicing fleet teleport; its secondary will be aboard the ship.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DNS	DNS	DNS	DNS	DNS SEC
Activities, Platforms, Operational Environments		All			

Table 6-2. Naming Services Standards

Notes:

- The protocol for DNS is defined in Internet Engineering Task Force (IETF) Request for Comment (RFC) 1035.
- WINS (RFCs 1001, and 1002) is a Microsoft Windows 3.11, Windows 95, and Windows NT standard now widely used. However, Microsoft plans to migrate to Active Directory (AD) so WINS users should include plans for migration to AD in 1999 and beyond.
- DNS is IAB Standard 13, as profiled by MIL-STD-2045-17505

Examples:

USS Los Angeles:	ssn688.navy.mil and alias losangeles.navy.mil
USS Theodore Roosevelt	cvn71.navy.mil and alias tr.navy.mil or roosevelt.navy.mil
COMARFORLANT	cmfl.usmc.mil
USS City Of Corpus Christi	ssn705.navy.mil and alias cityofcorpuschristi.navy.mil
Commander ASW Forces Pacific	cafp.navy.mil and alias ctf12.navy.mil
COMCRUDESGRU FIVE	ccdg5.navy.mil

6.3.2 Directory Service

Best Practices

Use a two-tiered directory structure as defined within the Distributed Computing Environment (DCE). For local references, use a Cell Directory Service (CDS) and connect multiple local services to a Global Directory Service (GDS). GDS is implemented using X.500 (ISO 9594) or the Internet DNS. To enhance application portability in an environment implementing multiple directory technologies with diverse naming conventions, use X/Open Federated Naming (XFN) and Lightweight Directory Access Protocol (LDAP) as the access mechanism. LDAP has become a de facto standard as it is currently supported, or planned to be supported, by most electronic messaging and Web enabled applications.

Applications that have requirements for a full function directory service will conform to the X.500 directory standards. Applications that require a naming service should select a naming system that integrates with a directory (X.500) system.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	X.500 LDAP	X.500 LDAP	X.500 LDAP	X.500 LDAP	
Activities, Platforms, Operational Environments		All			

Table 6-3. Directory Service Recommended Implementations

Notes

- X.500 is the leading standard for directory services.
- The X.509 standard (the ITU recommended standard for Digital Certificates) should be fully supported in any selection of an X.500 directory system.

- Select an X.500 directory system and schema that are compatible with the DMS X.500 directory.
- Implementations should support interfaces from multiple network applications.
- LDAP access to the directory must be provided and it should be compatible with and accessible from popular e-mail clients.
- Directory updates can be very bandwidth intensive. Ships with limited bandwidth should always update their directories the day prior to getting underway.
- Directories should be maintained at multiple teleports to ensure proper service level for ships transiting different ocean areas.

Guidance

Most vendors support interoperable solutions for directory services and naming. While most directory data used today reside in integrated, vendor proprietary messaging and file systems, the transition to an X.500 environment with access via LDAP is the preferred implementation. As long as the back-end X.500 directory system is scaleable, most systems that implement LDAP as the access technology are sufficient.

Much thought needs to be given to how the directory schema is created and how the distributed directory server architecture is implemented. Refer to the DMS X.500 Directory Service Implementation Guidance (Draft) which provides the Schema, the policies and procedures for implementing the DMS Directory Service, as well as other information including the management of the directory service and the functions required to ensure an effective directory service.

Given the complexity and time frames associated with the DMS directory, it is recommended that DON maintain its own enterprise directory. Initially, this directory might be used to hold basic personnel information (e.g. Command, address, phone number) but would also be used to keep track of individual's SMTP addresses. This directory should be implemented using X.500 standards and be accessible via LDAP capable (e.g. Web browser) clients. An implementation of the directory would likely have multiple, fully replicated instances, and be located at strategic DON points of presence. Collocation with ITSCs would be a logical option. The directory service that currently exists at "directory.navy.mil" provides a good example of how the directory might be organized.

It is recommended that individuals be given the capability to access and update their individual records and that organizations be given the ability to perform "bulk" uploads and/or changes if necessary. Most commands and organizations will maintain their own directories for the purpose of resolving internal resource lookups, so complete or partial replication of the DON directory into these local directories should be made possible. The DON directory should also provide the mechanism to store X.509 v3 certificates as necessary for certain personnel.

For messaging, many systems have the ability to create and maintain an X.400 Originator/Recipient (O/R) address for all recipients in the MHS. This address identifies a mailbox recipient in the global X.400 (DMS) address space. The following table displays those X.400 attributes that should minimally be associated with DON electronic mailbox recipients in a directory.

X.400 Attribute	MHS Value
County (C)	US
Administrative Domain(A)	“ “ (blank)
Private Mgmt Domain(P)	ORGANIZATION
Organization (O)	ORGANIZATION
Organizational Unit (OU)	(e.g., NAVSEA, CINCLANT)
Common Name (CN)	TBD
Generational qualifier (Q)	TBD
Initials (I)	Initials
Surname (S)	Last Name
Given name (G)	First Name
Domain-defined attributes	TBD

Table 6-4. X.400 Address Attributes

6.4 Public Key Infrastructure (PKI)

A public key infrastructure is a collection of components that support the generation and distribution of digital certificates, issuance of certificate revocation lists (CRLs), and the building and running of directories to serve these certificates and CRLs. In order to understand the operational issues and to develop the proper policies associated with operating a PKI, a number of Naval, DoD, and other government entities are operating PKI pilot projects based on commercial standards. These pilots are called “medium assurance” PKI pilots based upon the level of assurance postulated in the digital signatures associated with the certificates. The Defense Message System (DMS) project is fielding a separate PKI based partially on commercial standards and partially on DMS unique standards (this pilot project is sometimes called a “high assurance” PKI).

A digital certificate is an electronic proof of identity that can be used to sign electronic documents, to authenticate the holder of the certificate, and to allow decryption of information intended to be read by the holder of the certificate. Digital certificates are used in many commercial products (e.g., SSL for WWW security, S/MIME for e-mail security) and are based on the use of public key cryptography. In a public key cryptographic system, a person (e.g., using a web browser) generates a public key/private key pair. The private key is never revealed to anyone and is protected by the application that generated it (in our example, the browser). The public key can then be published (e.g., in an X.500 database). It should be noted that PKI identities should also account for the use of command/staff e-mail accounts.

A complete description of PKI and associated standards guidance is provided in Section 3.5.

6.5 Electronic Messaging and Attachments

Electronic mail (e-mail) message handling systems (MHS) are integral to enterprise computing strategies. E-mail implementation for the Navy and Marine Corps must conform to both the Simple Mail Transfer Protocol (SMTP) and to the international e-mail messaging (X.400) for compliance with DMS. The e-mail implementation strategy must also maintain enterprise connectivity of dissimilar e-mail message handling systems until they can be migrated to a common standard.

A Message Handling System is the name of a methodology to exchange electronic messages between originators and recipients. Both SMTP and X.400 are implementations of an MHS. An originator is an entity (i.e. a person or computer program) that sends or originates a message. The recipient is another entity, a person or a computer program, that receives the message. Certain requirements should be satisfied when providing a message exchange service between an originator and recipient.

- The message must not get lost or be altered in transit. In order to ensure this, MHS defines the transfer rules according to which the message is passed from one messaging switch or entity to another messaging switch or entity.
- The handling entities must be able to interpret the message. This includes the originator and the recipient, as well as the message switches handling the message in transit, which need to route the message and perform tasks relevant to the transmission of the message.

Most good message handling systems should be able to provide more than these basic minimum features. For example, the originator may wish to know when the recipient receives the message. In this instance, the originator might require that they be notified if the recipient cannot receive the message, because, for example, the address specified by the originator was erroneous. These MHS features or capabilities are commonly referred to as service elements.

SMTP and X.400 share a number of common service elements, most of which are duplicated and extended in vendor proprietary MHS. In fact many vendor proprietary systems utilize either SMTP or X.400 as a baseline upon which they add additional service elements.

Standard Messaging Application Program Interfaces (MAPIs) provide access to directory services, message profiling, message store-and-forward capabilities, and electronic transport capabilities of message handling systems. A message type called X.435, present in the 1988 version of X.400, provides standardized support for Electronic Data Interchange (EDI) transaction transport and interchange over communications networks. This EDI message type facilitates the movement, delivery, and security of EDI transactions over X.400 networks.

To date, the interfaces between the DMS architecture and other related DON efforts involving messaging, such as IT21, have not yet been defined. For example, DMS has selected X.400 and X.500 for messaging and directory protocols while most of the industry is trending towards SMTP and LDAP. A “flexible architecture” approach for DMS implementation has tentatively been established to address these issues. A concept for the DON DMS flexible architecture has been proposed to establish the originally designed DMS application installed in the DII and within the DON infrastructure (Section 6.3). Other efforts could interface to this backbone to relay command messages and e-mail to commands (including ships, aircraft, submarines, mobile tactical units, and small shore commands). Existing COTS based software would allow for exchange of mail between the core DMS protocols (X.400/X.500) and Flexible Architecture Protocols (SMTP/LDAP).

The ultimate goal is to have a convergence in the tools that the DON uses to perform messaging. However, a distinction is necessary between the notion of “command correspondence” (e.g. JANAP 128 for GENSER or DOI 103 for SCI) and “personal messaging.” This distinction is primarily one of doctrine and procedures on how the messaging system is used versus the technologies used to construct the messaging system.

Best Practices

Choose electronic message handling systems that conform to Internet based (SMTP) standards as well as the international e-mail messaging (X.400). The chosen e-mail message handling systems should add Application Program Interfaces (APIs) to the basic e-mail message handling system services such as message store-and-forward and electronic transport.

For DMS compliant organizational messaging, products should be chosen that support the DMS standards. Messaging that requires elements of service unique to the DOD will use X.400 (DMS) protocols. Examples of such services include guaranteed delivery, timely delivery within tight time constraints, auditing, and alternate routing capabilities.

Secure Multi Purpose Mail Extension (S/MIME) is the preferred encoding for attachments. S/MIME requires use of an established Public Key Infrastructure (PKI) for issuing and revoking security certificates. Use of MIME is acceptable until a DON enterprise PKI is established. Because many of the most critical communication links are bandwidth limited, users should compress attachments whenever possible. ZIP 2.04 (or higher version) compression protocol should be used to compress all attachments.

Commercial versions of DMS compliant messaging systems should be selected for electronic messaging solutions and should be interconnected with SMTP and X.400. Messaging that requires only minimum essential elements of service would comply with a standards profile based on SMTP/S/MIME, LDAP, X.509(V)3, and IMAP-4 client to server interface standards. These standards likely address the majority of messaging needs throughout the DON. Post Office Protocol (POP3) services must continue to be provided until a transition to IMAP4 is complete.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	SMTP X.400 (1992) POP 3 IMAP 4 MIME RFC 1521 S/MIME RFC2312 ZIP 2.04	SMTP X.400 (1992) POP3 IMAP 4 MIME RFC 1521 S/MIME RFC2312 ZIP 2.04	SMTP X.400 (1992) IMAP 4 MIME S/ MIME RFC 1521 ZIP 2.04	SMTP X.400 (1992) IMAP 4 MIME S/ MIME RFC 1521 ZIP 2.04	X.435 ESMTP
Activities, Platforms, Operational Environments		All			

Table 6-5. E-mail with Attachments Recommended Implementations

6.5.1 Implementation Guidance

- Select suppliers who support X.400, SMTP and the capability to handle compound documents between them.
- Support for the Multipurpose Internet Mail Extensions (MIME) and the Secure Multipurpose Internet Mail Extensions (S/MIME) standards should be included in any MHS solution.
- Post Office Protocol 3 (POP3) and International Mail Access Protocol (IMAP) do not constitute fully functional MHS, however POP3/IMAP access to a robust messaging solution may be appropriate in some situations. Choose an MHS that supports both standards now, but plan to phase out POP3 in favor of IMAP when practical.
- Avoid non-X.400-compliant messaging systems in 1999 and beyond. Explore the use of ESMTP when it becomes available.
- Products should, whenever possible, use X.500 for all naming and directory services and must support the Lightweight Directory Access Protocol (LDAP) standard for directory access.
- Select suppliers who have scaleable and manageable SMTP solutions that comply with IAB STD 10 (including RFC 821, SMTP, and the service extensions identified in RFC-1869 AND 1870).

6.5.2 Selection of an E-mail System

A handful of vendors have “enterprise class” solutions that can support organizational (i.e. DMS) as well as interpersonal electronic messaging. Using products available on the DMS contract, a significant number of DON customers have already made their e-mail system selection. In order

to reduce the cost and complexity of supporting different e-mail systems within a command, it is desirable to select an e-mail product that can address both the organizational and interpersonal messaging requirements. In addition, it is also prudent to be aware of the e-mail systems already selected by other DON commands – system homogeneity will facilitate communication with other DON commands. As with any other complex system, e-mail system selection should follow the guidance provided in section 2.9. Along with command functional requirements, DON wide security and seamless interoperability are two other overriding factors to be considered. Because it is a foundation technology that forms the core of DON Information Distribution, e-mail system homogeneity will be a driving factor in the push to reduce complexity and Total Cost of Ownership (TCO) within the DON. It is worth reiterating that care should be taken when selecting e-mail products that do not support both personal and organizational e-mail and where this decision deviates from mainstream DON products.

6.5.3 E-mail System Implementation

The requirement for DON e-mail systems to seamlessly interoperate suggests that the ITSG should provide guidance so that implementations throughout the Navy and Marine Corps are consistent and realize the full benefit of system features. The network operating system used to support the e-mail system implementation should be configured to support maximum flexibility and portability within the DON. It is desirable that commands moving between satellite footprints and those commands embarking aboard ships have continuous and seamless access to their resources (e.g. accounts, printers, and servers). This will necessitate significant DON collaboration on network operating system naming schemes, hierarchies and trust relationships. Since the e-mail system implementation is closely tied to the network operating system implementation, DON-wide collaboration on e-mail system naming and hierarchy is also required to ensure maximum interoperability. Where possible, resource naming should follow the same naming conventions as provided for DNS in Section 6.3.1. The standard fill for the e-mail system user accounts is suggested in Table 6-6.

E-mail System Data Element	Description
Last Name	User's Last Name
First Name	User's First name
Company	Full Name of the Command
Title	Rate and Rank of the User
Department	Command Department or Single Digit Staff Code (e.g., N3)
Office	Title of the Officer, Command or Staff Position, Staff Code

Table 6-6. Standard User Directory Fill

6.5.4 Interoperability with Other E-mail Systems

Because of the dynamic nature and current heterogeneous state of DON electronic messaging and the difficult realities of implementing a single, coordinated messaging solution across the entire DON, it is recommended that SMTP be used as the interconnection backbone.

Through the use of a DON-wide mail switches it should be possible to have a messaging clearinghouse that, coupled with a robust DON wide directory, would be able to process mail for any DON e-mail system in the interim period until DMS becomes operational. This mail switch could also serve as a DMS Multi Function Interpreter (MFI).

6.5.5 Individual's Official E-mail Address

In combination with the master Navy and Marine Corps X.500 directories and the mail switch, the DON directory would be used to dynamically map this address to the multiple changing addresses that users will inevitably have as they change codes or move to other organizations. Note that such a switch system would not preclude organizations from directly interconnecting their respective messaging systems nor would it interfere with the instance where the actual SMTP address of a user is specified.

Each DON user would have at least one SMTP address that follows them independent of the command or organization where they are employed. This address will be referred to as the user's Official Individual Address. The address would take the form of "username@navy.mil" or "username@usmc.mil" and would "follow" its owner throughout his career, independent of duty station.

6.5.6 Display Name

The standard display names for members of your own command should be the following format:
`STAFF CODE – RATE/RANK First Name Last Name`
For example:
`N32 – LT James Jones`

For entries away from the command, the same format should be used except preceded by an abbreviation of the command name.
`COMMAND STAFF CODE – RANK/RATE First Name Last Name`
For example:
`SSN688 OPS LCDR Jim Jones`

For commands where it is inappropriate or confusing to use the staff code to sort display names the following format should be used:
`Last Name First Name (MI) RATE/RANK`
For example:
`Smith, Tom P LCDR`

6.6 Network Utility Services

The following services are needed to monitor, troubleshoot and maintain the network. These services are used by the system administrator and should not be accessible to the operator.

6.6.1 Network Time Service

Time services are established to ensure consistency and accuracy of time and dates across distributed systems. Synchronization is a special problem in networks of multiple hosts because each host has its own clock and its own time reference. Slower clocks continually drift further behind faster clocks. Time skew among networked hosts can cause application delivery problems. For example, a stock trading wire service could be in trouble if brokers in London learned of

deal-making events five minutes after brokers in New York or Hong Kong had already acted. Moreover, time synchronization is critically important to sensor data fusion in C4I and weapon systems.

The DCE Distributed Time Service (DTS) minimizes such situations by synchronizing host clocks in LANs and WANs. Clock synchronization enables distributed applications to determine the sequencing, duration, and scheduling of events, independent of where they occur.

DTS servers synchronize themselves by obtaining time information from all other DTS servers on the LAN. Global servers provide synchronization for servers on extended LANs. DTS alone ensures that DCE hosts share a consistent notion of time. This time, however, is not necessarily the correct time. Servers can be synchronized with external time standards by setting the time manually or by connecting to an external time provider.

The US Naval Observatory is a recognized time reference custodian. DTS uses the Coordinated Universal Time (UTC) standard, which has largely replaced Greenwich Mean Time as a reference. Many standards bodies disseminate UTC by radio, telephone, and satellite. DTS has a Time Provider Interface (TPI) that describes how a time provider process can pass UTC time values to a DTS server and propagate them through a network. The TPI also permits other distributed time services, such as the Network Time Protocol (NTP), to work with DTS. UTC is referenced to a set of atomic clocks and is a proper reference for time synchronization purposes. GMT is referenced to earth's rotation which is several orders of magnitude more variable than the atomic clocks. GMT is adjusted to less than half-second differences to UTC by adding leap seconds either 31 Dec or 30 June as necessary.

Loran and Global Positioning Systems (GPS) receivers provide excellent primary reference and also provide worldwide time services, however, Loran time receivers are a bit more stable because they do not have to contend with selective availability. DTS is transparent to DCE users, but users cannot access DTS directly. Applications can, however, use the time functions available from the DTS API. For example, an application for conference call scheduling can get time zone information from the DTS API to determine the best times to schedule conference calls that span multiple time zones.

Best Practices

For an application that needs the correct time, use either the POSIX.1 time to get a simple scalar with an unknown accuracy or use the DTS API to get the interval time stamp.

Use NTP (RFC1305) and TOG DCE DTS time protocols. TOG DCE DTS supports the synchronization of time with an external time provider, such as Internet time providers, that uses the NTP protocol. Since the NTP is an inherently insecure protocol, it should not be permitted outside of the Zone 4 firewall. If an appropriate time source cannot be found inside of the Zone 4 security boundary, (e.g. DTS) then configuration of a GPS based time source inside of the boundary is appropriate.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DCE DTS NTP	DCE DTS NTP	DCE DTS NTP	DCE DTS NTP	
Activities, Platforms, Operational Environments		All			

Table 6-7. Network Time Service Recommended Implementations

Notes:

- DCE's Distributed Time Service is a transparent method of obtaining time services that are highly synchronized.
- Network Time Protocol (RFC1305) is a simple method of obtaining time across a network, provided a server is available.

Guidelines

NTP server implementations are publicly available, either bundled in the operating systems or available for download. Many DON combatants have systems onboard which could be used to drive an NTP server; all have a GPS and or Loran receiver with which to cross-check and update. In the right circumstances, it is appropriate for some ships to implement a time-server, and at least one Stratum One clock on NIPRNET can be used as a reference.

6.6.2 System Management Services

System management services permit monitoring, control and management of system objects. The full complement of system management services are covered in Chapter 10. The two primary specifications that support network management are the Simple Network Management Protocol (SNMP) and the Remote Network Monitoring, version 2 (RMON 2).

Best Practices

Use management systems and protocols that minimize non-payload overhead and that can be assembled into an integrated system to control and monitor all aspects of the entire infrastructure from a single workstation.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	SNMPv1 RMON 2 XSM	SNMPv1 RMON 2 XSM	SNMPv1 RMON 2 XSM	SNMPv1 RMON 2 XSM	DMI WBEM
Activities, Platforms, Operational Environments		ITSCs and Shore. Bandwidth consumption must be considered prior to use for Ships, Ground, and Aircraft			

Table 6-8. System Monitoring and Control Recommended Implementation

Notes:

- Simple Network Management Protocol (SMNPv1) has some denial of service security concerns that need to be compensated for by other means.
- Remote Network Monitoring (RMON 2) provides comprehensive system management at or above the network layer.
- Desktop Management Interface (DMI) provides for management of server and personal workstation resources.
- Web Based Enterprise Management (WBEM) is an emerging specification that allows multiple system management access using a Web-based interface.

6.6.3 Remote Access Services

Remote access services are primarily covered by System Management Services and Telnet. Telnet allows remote access of system devices and computers. Its use should normally be disallowed but many legacy applications and systems necessitate the use of Telnet. If used, it should be appropriately proxied and limited only to the necessary personnel.

6.6.4 File Transfer Services

File transfer services let users copy, replicate, or move whole files across a network. TOG and ISO standards help provide standards for this service across a heterogeneous network of conforming systems. In addition, the de facto standard File Transfer Protocol (FTP) is an industry-prevalent mechanism found in most TCP/IP implementations.

Although FTP is a specialized means of transferring files, electronic message handling systems can also be used for transporting files. A standard called Multipurpose Internet Mail Extensions (MIME), which has emerged from the Internet mail protocol (SMTP), permits various file types to be transferred as attachments to messages. All mail systems have limits on the size of files they can transfer; some are as few as 32 KB (kilobytes).

Most network operating systems have file transfer capabilities integrated into their file systems that make network file transfer as easy as dragging and dropping files from one folder to another. Rarely are these proprietary systems useful outside their local implementation domain and those

that have that functionality tend to pose unsatisfactory security risks. Moreover, these systems are notoriously inefficient from a networking standpoint, especially over low bandwidth channels.

The use of the Hypertext Transfer Protocol (HTTP) continues to open up new opportunities to construct file transfer systems across multiple networking environments and systems. Coupled with file compression and “push-technology”, this de facto, open standard may also provide file transfer capabilities to bandwidth challenged environments. As HTTP continues to become embedded in desktop and server operating systems, use of its file transfer mechanism is likely to increase.

Current tools and methods assume that any encryption requirements are handled before and after file transfer. Future implementations are expected to integrate encryption support or be compatible with a Public Key Infrastructure (PKI) implementation of X.500/509.

Best Practices

Select file transfer systems that conform to open standards and promote interoperability. The electronic messaging method of file transfer should only be used for small files (already compressed using ZIP), ideally less than 5 MB. Files larger than 5 MB should be transferred using the Web Drop and Pickup Service (Section 6.2.8).

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary file transfer systems	HTTP FTP MIME RFC 1521 S/MIME RFC2312	HTTP FTP MIME RFC 1521 S/MIME RFC2312	HTTP FTP MIME RFC 1521 S/MIME RFC2312	HTTP FTP MIME RFC 1521 S/MIME RFC2312	
Activities, Platforms, Operational Environments		All			

Table 6-9. File Transfer Service Recommended Implementations

Notes:

- Use file transfer system implementations that are based on the Internet Protocol (IP) standard
- SHTTP is a more secure version of HTTP that provides a basic level of encryption of data for data traveling between the client and server

6.6.5 Electronic Dialog

Along with Network News Service (Section 6.8), electronic dialog can be accomplished using Internet Relay Chat (IRC). There are many applications for a running type dialog such as system troubleshooting over small bandwidth links.

6.7 Web Services

A "web" is a collection of servers on a network that communicate with web browsers using the Hypertext Transport Protocol (HTTP). The most famous web is the World Wide Web, which is the collection of web servers publicly available on the Internet. The browser sends an HTTP request to a web server for a Hypertext Markup Language (HTML) document. After receiving the document, the browser displays it to the user. An HTML document can contain text, graphics, and links to other documents or to different sections of the current document in the form of Uniform Resource Locators (URLs). An HTML file can also contain embedded within it audio files, video files, 3D graphics, Virtual Reality Modeling Language (VRML), or other document types. Further, an HTML document can contain its own locally executed instructions (scripts) for simple activities or full-blown applications in the form of Java applets or ActiveX objects. A link can refer to a Common Gateway Interface (CGI) which supports additional functionality on the server side of the connection, e.g., a database interface or added security processing.

6.7.1 Web Servers

A web server is any computer on a network that is running Hypertext Transfer Protocol (HTTP) server software. HTTP can be used to move any kind of data over a TCP/IP network between a web server and a web browser (client). HTTP is a transaction-oriented client/server protocol.

Even though there are many document formats/protocols listed in Section 6.7.2 (Web Browser), the web server, which only needs to speak HTTP is serving them all. HTTP is the dominant protocol (majority of network traffic) on the Internet, as well as on many dedicated DoD networks.

In addition to serving up HTML pages to the clients, the HTTP server must support Common Gateway Interfaces (CGI). CGI is an Application Program Interface (API) that supports server side processing, i.e., the execution of applications on the web server or another machine for which the web server is acting as a front-end. Examples of server side applications include processing HTML forms, dynamic document generation, and providing access to database servers. CGI scripts are typically written using UNIX shell scripts, Perl, TCL/TK or C, but can be written in almost any programming language (see Chapter 9 for development tools and languages).

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	HTTP 1.0 SSL	HTTPv1.1 SSL	HTTP-NG SSL	HTTP-NG SSL	
Activities, Platforms, Operational Environments		All			

Table 6-10. Web Service Recommended Implementations

Notes:

- HTTP is the standard of the Internet Engineering Task Force, the current release version is HTTP 1.0, however, HTTP version 1.1 is IETF proposed standard RFC 2068 and is currently undergoing public review.
- HTTP 1.1 is designed to bring about significant performance gains through support for persistent connections and pipelining for much more efficient use of TCP networks, continued extension of the caching model and support for multi-homing servers (allowing a single web server to serve multiple web sites each with their own unique address). Improvements in HTTP 1.1 are limited due to the requirement for backwards compatibility with HTTP 1.0.
- HTTP-Next Generation (HTTP-NG) is an on-going effort to redesign the HTTP protocol for greatly increased efficiencies.
- Secure Sockets Layer (SSL) is an extension to HTTP that provides for user authentication, added privacy and assurances of data integrity.

Guidelines

A web server is a very public resource that must be well maintained with regard to security vulnerabilities to prevent compromise resulting from publication of erroneous data or denial of service.

There are a number of tools that make administering a web server significantly easier, see Section 6.7.3, WWW Utilities, for more information on these.

Web servers are often sold as suites that can include a message (e-mail) server, a directory server (typically LDAP), a data push content server, a streaming audio/video server, and text search services. Standards and functionality for these functions are addressed elsewhere in this document. Significant cost savings on purchase price and integration can be afforded by buying bundled server suites.

Network performance can be significantly affected by the use of effective caching schemes between the client and server to prevent the repeated download of pages from the server that exist on the client cache and have not changed.

6.7.2 Web Browsers

The web browser or client is primarily the local user's viewer for documents provided by the HTTP server. The browser is now evolving to be the main, or sole element of the presentation

layer of many system architectures. The web browser provides an easy-to-manage, universal client interface for display of text, graphics, multimedia, and forms-based data. The browser's native data display capabilities can be extended through the use of external "helper" applications or Java applets to support graphics-intensive or real-time data display requirements.

The web browser's native language is Hypertext Markup Language (HTML). HTML is a platform independent "tagged" language that is both human and machine readable and can be transmitted as straight ASCII data. The current version includes support for advanced forms, in-line frames, enhanced tables, support for objects and scripts, style sheets and more.

A key browser technology that was originally handled by "helper" applications, but which is now being built into browsers is Virtual Reality Modeling Language (VRML). VRML will realize increasing use for 3D user interfaces and has great potential for military applications.

Another browser extension with excellent military potential is variable resolution still images. This technology delivers higher-resolution images only as they are needed, minimizing network bandwidth demands while enabling a user to pan and zoom on an image. Use of this technology can also greatly improve print quality by downloading a higher resolution version of the image when printing (computer screen display is at 72 dots per inch while printers typically require 150 to 300 dots per inch). The initial commercial implementation of this technology is FlashPix, an effort by Kodak, Hewlett-Packard, Live Picture and Microsoft. FlashPix is built on top of the new Internet Imaging Protocol (IIP) - defined by Hewlett-Packard and endorsed by Netscape and Microsoft. IIF enables a plug-in, applet or helper application to interactively request image and property data from a web server. For example, a client can request just a section of an image. IIF was designed for FlashPix but it works with Graphics Interchange Format (GIF) and Joint Photographic Experts Group (JPEG) images also.

6.7.2.1 Evolution of HTML

There are many initiatives under way to extend or replace HTML as the demands being placed on the web interface grow beyond the display of simply formatted static documents. These initiatives are under the auspices of the World Wide Web Consortium - the industry/education partnership that controls most WWW standards.

The need for more complex document formatting led to the development of Cascading Style Sheets (CSS). CSS allows a page author to specify a much more precise document formatting template that is automatically applied to the entire document instead of requiring manually set display attributes for every element of the document (http://www.w3.org/areas.htm).

The desire for more interactive web pages led to the creation of Dynamic HTML. Dynamic HTML is a set of technologies that expose HTML attributes as properties that can be manipulated by scripts. DHTML is complex to produce manually but there are increasing numbers of HTML editors that support it. Using DHTML is made more difficult by the differing implementations on Netscape Navigator and Microsoft Internet Explorer.

DHTML is built on top of the Document Object Model (DOM) which is "a platform- and language-neutral interface that will allow programs and scripts to dynamically access and update the content, structure and style of documents" (http://www.w3.org/areas.htm).

The eXtensible Markup Language (XML) is the proposed ‘follow-on’ to HTML. XML is based on the Standard Generalized Markup Language (SGML), ISO Standard 8879, tailored for the

WWW. "XML is primarily intended to meet the requirements of large-scale Web content providers for industry-specific markup, vendor-neutral data exchange, media-independent publishing, one-on-one marketing, workflow management in collaborative authoring environments, and the processing of Web documents by intelligent agents" (http://www.w3.org/Press/XML-PR.html).

The major key feature found in XML is that it allows publishers to define their own markup language using application specific meanings. This would enable an author to build mathematical equation structure; automatic database updates with schemas intact; integrated meta information system structures; XML protocol enabled selectively address and download of portions of XML documents; and new animation, scripting, object model, style sheets, automation, and printing functionality.

Channel Definition Format (CDF) is XML extension proposed by Microsoft to define content and format for pushed (webcast) data.

6.7.2.2 Procedural Extensions

HTML is not designed to support procedural capabilities (i.e. the ability to execute application code or carry out some procedure). However, web pages can add procedural capabilities – primarily as extensions to the user interface - via client-side scripting or server-side scripting via embedded application parts or applets. The use of these proprietary extensions should be carefully controlled and the web development should adhere to HTML standards to ensure cross platform browser compatibility.

Client-side scripting includes small sections of program code stored in HTML pages that are interpreted by the client when the page is loaded. Client-side scripting is done in JavaScript (based loosely on Java) or VBScript (based on Visual Basic).

Server-side scripting is discussed in Section 6.7.1 (Web Servers).

Application parts are either ActiveX parts or Java applets. ActiveX parts are embeddable program objects, typically written in Visual Basic, but they can be in C or Java. Java is an object-oriented programming language based on the C programming language. Java can be used to program either conventional stand-alone applications or small downloadable applications called "applets." The partially compiled source code (called bytecode) for an applet is embedded in the HTML document. When the document is downloaded from the web server, the Java bytecode is automatically executed by the system or browser's Java Virtual Machine.

6.7.2.3 Extension of the Web Browser as an Application Interface

In the personal computer world, there is an increasing blurring of the lines between the browser and the operating system top-level interface or "desktop." Microsoft, in particular, is pushing the total integration of Internet Explorer with the Windows95 and Windows NT desktop through their Active Desktop product. Regardless of how that effort turns out, the browser will provide building blocks for developers to easily create user interface functionality. The various user interface and control elements of the web browsers are being turned into programmable objects. For example, both Internet Explorer and Netscape Navigator include e-mail programs that support HTML formatted electronic mail by embedding the browser's display functionality in the mail application. This technical direction will be enhanced with the release of web browsers that are written entirely in Java.

Netscape has created a Resource Definition Framework (RDF) that allows for the creation of a metadata layer of the underlying data stores of Netscape Communicator - allowing users to customize the user interface. RDF is based on the eXtensible Markup Language (XML). Netscape also plans to expose the Communicator APIs as JavaBeans and scriptable components, allowing developers to create applications built on top of these capabilities. Netscape will also make available to developers a new rendering engine (code-named Gemini) that supports HTML, XML and other formats that developers can embed directly into their own applications.

There is currently no standard set of APIs or object interfaces for manipulating all browsers.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	HTML 4.0	HTML			XML
	Java	VRML			PNG
	JavaScript				PICS
	VRML 2.0				RDF
	Quicktime VR				SMIL
	Quicktime				RTP
	AVI (MPEG-4)				RTSP
	SSL				IIP/Flashpix
					SETP
					DOM CSSI
					CDF
Activities, Platforms, Operational Environments		All			

Table 6-11. Web Client Recommended Implementations

Notes:

- Several of these standards duplicate standards included in Section 6.3.1 (Web Servers) because the web server and the web client must speak the same protocol for those protocols involved in communication between the client and server.
- W3C released HTML 4.0 as a "recommendation" on 12/18/97 (http://www.w3.org/Press/HTML4-REC, 1/11/98, 9:02PM). There will be a transition from the current HTML 3.2 standard to HTML 4.0. Browsers and development tools that support HTML 4.0 are currently available, however all features of HTML 4.0 are not supported by all web browsers.
- eXtensible Markup Language (XML) 1.0 is a "proposed recommendation" being voted on by W3C membership for consideration as a "Recommendation."

- Java applets are supported by both leading browsers (Navigator and IE); ActiveX support may not be available on all platforms. Java applets should be written in "100% Pure" Java code - not using Microsoft specific extensions.
- JavaScript is supported by both leading browsers (Navigator and IE); VBScript is only supported by Microsoft.
- VRML 2.0 supports 3-D rendering of navigable spaces plus encapsulation of images, animation and audio. VRML supports "hot spots" - allowing a developer to embed hyperlinks to other HTML or VRML documents or embed other programming languages so objects can be assigned behaviors.
- QuicktimeVR supports 3D navigable spaces that are composed of 360 degree panoramic photos which can be navigated similar to VRML.
- Quicktime is a multimedia data format for synchronized media (sound and video) that is cross-platform and popular.
- AVI - digitized video data format popular in the personal computer world.
- Portable Network Graphics (PNG) - W3C initiative to develop an improved bitmap graphics format that addresses limitations of current formats (http://www.w3.org/areas.htm).
- Platform for Internet Content Selection (PICS) - W3C specification provides for labeling of web site content. While this is primarily used today to provide access restrictions for children on the Internet, there are potential applications for this technology on Navy sites (http://www.w3.org/areas.htm).
- Resource Definition Framework (RDF) - PICS is at the heart of an expanded "metadata" effort at the W3C to provide a standard way to describe the properties of web pages - including providing data for access controls, copyright restrictions, additional security functionality and improved content indexing (http://www.w3.org/Metadata/activity.html).
- Synchronized Multimedia Integration Language (SMIL) is a W3C initiative to language for controlling "continuous multimedia presentations" where audio, video, text and images must be presented in a synchronized relationship. The first public draft for SMIL was released by the W3C in November 1977 (http://www.w3.org/audiovideo/activity.html).
- Real Time Transport Protocol (RTP) - protocol for streaming data (audio and video) applications developed by the Internet Engineering Task Force (IETF). (http://www.w3.org/audiovideo/activity.html. Also see http://www.ietf.cnri.reston.va.us/home.html for more information.)
- Real-Time Streaming Protocol (RTSP) - protocol under development by the IETF, that builds on HTTP technology (caching, authentication, encryption), for streaming data (audio and video) applications (http://www.w3.org/audiovideo/activity.html. Also see http://www.ietf.cnri.reston.va.us/home.html for more information.)
- Internet Imaging Protocol (IIP)
- Live Picture Inc., FlashPix image format, Realspace Image Server, FlashPix plug-in
- FlashPix technology was developed jointly by Kodak, HP, Live Picture and Microsoft
- Secure Sockets Layer (SSL) is an extension to HTTP that provides for user authentication, added privacy and assurances of data integrity
- Secure Electronic Transaction Protocol (SETP) - developmental security protocol designed to enhance the security of digital commerce transactions, supported by both Netscape and Microsoft
- Document Object Model - "a platform- and language-neutral interface that will allow programs and scripts to dynamically access and update the content, structure and style of documents. The document can be further processed and the results of the processing can

be incorporated back into the presented page." http://www.w3.org/areas.htm (11 January 1998)

- Cascading Style Sheets Level 1 (CSS1) is W3C recommendation
- Channel Definition Format (CDF) is XML extension proposed by Microsoft to define content and format for pushed (webcast) data. It has not yet been accepted by any standards organization.

Guidelines

Use of formats other than HTML for data distribution (i.e. Portable Document Format (PDF), Java) hides data from search engines and inconveniences users who have to wait for a plug-in or helper application to download and/or launch or wait for the Java applet to launch before they can view the document. Packaging data in these formats also discourages its reuse.

With the aggressive addition of new web browser features by both Netscape and Microsoft, adherence to the HTML standard provides the only guarantee of compatibility with all web browsers. Features beyond the current HTML standard should be used only when the user is certain that both vendors support the new feature. Even adherence to the HTML standard is not a guarantee that all users will be able to access all the functionality of a web site. A site developer must ensure that the entire target audience has, or will, upgrade their browser to the version that supports the current HTML standard or added feature before fielding new HTML features.

Both Netscape and Microsoft make their browsers available as part of a larger suite of integrated applications. If an organization has already paid a license for this suite of software and is going to install the shared code necessary to run the web browser, there are cost efficiencies in using the remaining elements of the suite. This should be taken into consideration when evaluating products for e-mail clients, newsgroup readers, data push solutions, HTML editors, directory services clients and collaboration tools. If the bundled solutions are not to be used by the organization then steps should be taken to prevent their use as an alternate to the approved standard application.

6.7.2.4 Browser Security

In addition to the security protocols identified in the Recommended Implementation section, here are some other general web browser security notes.

The security of Java applets is addressed by the “sandbox” restrictions built into the Java language.

A web browser gives the end user the ability to download and open files directly in an external application (for example Microsoft Word). Most current virus protection software will not catch an infected document that is not saved to the disk first and then opened by an application. There are commercial products that claim to support this, either web browser anti-virus plug-ins or continuous background virus checkers that are supposed to intercept files once downloaded. Web technologies and products should be subject to careful security evaluation prior to deployment and tight configuration control once deployed.

The use of digital certificates is a key technology for positively identifying a web browser user to a web server. Certificates surpass passwords in providing strong security by authenticating identity, verifying message and content integrity, ensuring privacy, authorizing access, authorizing transactions, and supporting non-repudiation. Digital certificates are discussed in more detail in Section 3.5, Public Key Infrastructure.

6.7.3 Web Utilities

There are necessary capabilities beyond web servers and browsers that make it possible for the web to work. These include HTML editors, web site content management tools, web site scripting tools and languages, site usage tracking tools, web server management tools, site watchers and site grabbers.

6.7.3.1 HTML Editors

There are a large variety of What-You-See-Is-What-You-Get (WYSIWYG) web page editor applications available with the goal of allowing any user to created HTML documents without having to actually write HTML. Each of the leading browser packages include a basic HTML editor (Microsoft FrontPage Light, Netscape Composer), however there are other products available which provide additional functionality. Any tool selected should support:

- WYSIWYG frames page editing
- basic image manipulation (resize, brightness and contrast adjustment, transparency)
- image map creation (definition of hotspots and associated URLs)
- easy table creation
- linkage for document preview in a web browser
- support for automatic generation of navigation bars and other shared page elements
- the ability to apply a consistent style or "look and feel" to a collection of web pages

Any tool selected should also support new features as they are added to the appropriate web standards and as the leading browsers implement them. It is worth noting that many (today), and eventually most (soon) office productivity applications have an "export to HTML" capability, making them advanced HTML editors of a sort.

6.7.3.2 Web Site Content Management

While most any user is capable of generating HTML documents, most are not capable of managing a web server. The most frequent day-to-day activity involved in web server or "site management" is updating the content of the server. There is now a class of tools typically referred to as "site managers" that provide a graphical user interface for adding and deleting files from web sites, moving elements of the site around (and automatically updating the changed links), link validation (to find broken links), and migration of sites from one server to another.

6.7.3.3 Web Site Scripting Tools and Languages

Web pages can be extended to support a richer user interface or local application functionality through the use of procedural languages. There are two languages that can be applied at the document level (included in the document and interpreted at run-time) - JavaScript and VBScript. Other languages can be used to create application parts that are incorporated into a web page. These are typically implemented as Java applets or ActiveX parts. This is an area where there is conflict between the two leading browser vendors (Netscape and Microsoft) and not every browser supports all these technologies.

6.7.3.4 Site Usage Tracking

These are tools that allow non-real-time data analysis on HTTP server logs to identify who is accessing a web server and what sections of the server are being accessed.

6.7.3.5 Web Server Management

There are many functions that a web server system administrator needs to be able to perform. There should be some alert mechanism to make the administrator aware when web servers fail or reach specified traffic thresholds. For a heavily trafficked site, applying software tools that balance web server load across several web servers is a key approach to maintaining reasonable response times for users. The ability to test web server performance, to analyze traffic on local network segments to identify choke points, and the ability to monitor server activity in real time are all useful system administrator functions supported by these tools. Finally, the ability to identify all web servers on an Intranet is useful - especially for finding unauthorized web servers.

6.7.3.6 Web Watchers

These are tools that are typically applied at the individual user level to allow them to "register" pages on servers that they want to be notified of updates. Typically, when a page on a server being "watched" is updated, an e-mail is sent to the user announcing the update. This functionality can be provided by the site being monitored, but more frequently needs to be provided by a tool running locally. An ability to set up user bookmarks as "subscriptions" is included in Internet Explorer 4.0 and will probably migrate to other browsers. The subscribed sites are periodically checked for updates and the user can be notified through a change in the visual representation of the site's bookmark.

6.7.3.7 Site Grabbers

These are tools that are typically applied at the user level to simplify the process of downloading the multiple data elements (HTML and GIF images) that make up a document on a web server. These tools can also be applied at a command level to mirror outside sites - to speed access, ensure availability or to meet security constraints. The end user specifies what sites to download, how frequently and how many levels deep within the site to download and if the download should include links to sites outside the target site. Some tools also allow the user to specify the maximum amount of disk space a downloaded site snapshot can take up. Properly implemented, the site browser will go first to the local snapshot of an external site and see if the local information is current, before going out over the (typically slower) network to contact the site itself.

Best Practices

To be determined.

Recommended Implementations

There are no standards specific to these tools. The tools need to support the standards called out in the Web Server and Web Browser sections of this document. As preferences emerge, they will be provided in future DON ITSG releases.

6.7.4 Data Search and Retrieval

The web browser is increasingly becoming the standard or preferred interface for information presentation. Associated with that function, the web also serves as the interface and infrastructure for a wide range of data search and retrieval technologies that make data, especially from legacy systems, available to the end user.

These capabilities are typically made available through the use of a three tier or three layer architecture where the web browser is tier one, the HTTP (web) server and its associated applications (through CGIs) are tier two, and the database or other back-end server is tier three.

Data search and retrieval functionality can be broken down into three main areas - database access, web search engines and text search.

6.7.4.1 Database Access

Some experts predict that within two years, 80% of database queries will be over the web. The web typically provides easier to use interfaces at lower costs to an expanded user base. Database access is typically provided by using the web browser as the user interface which talks through the web server to an application called a "middleware" package that in turn talks to the database server. The goal of the middleware package is to hide the differences and details of the interface to the various database servers from the developer who is setting up the web interface to the database. The user interface for querying the database is almost always via a form the user fills in with search terms, and the results are normally either displayed in a form or as lists of links the user can select to get more detailed information.

6.7.4.2 Web Search Engines

Any user who has been on the World Wide Web should be familiar with the services provided by commercial web search engines like Yahoo! and AltaVista. This same functionality is available for implementation on Intranets. The end user provides one or more keywords or a phrase to search on and the search engine returns a list of sites that match the query. Various search engines support more complex queries, ranking the results based on the quality of the match to the query and various approaches to collecting and indexing information about sites.

Web search functionality can be divided into two main classes – web directories that provide an indexed structured view of sites based on site keywords and selected contents (like Yahoo!) and search engines that index the full content of web sites (as represented by AltaVista).

6.7.4.3 Text Search

Full-text and attribute-based searches support creation indexes of intranet and Internet information with browsable category tree interface. This is different than an unstructured text archive/search engine (Memex, Topic, etc.), that is also an essential function (especially for dealing with message traffic) that can typically be provided through a web interface. This information can be indexed in many native application formats (Office) as well as text and HTML. “Robots” are agents that traverse the net and collect information, submit to the search server for indexing and categorization, and then serve up to users (through search/browse managers). Live query can be conducted though single and multi-field keyword searches. There are no standards for any of this (other than HTML enabled mail for delivery of newsletters that contain links/URLs).

Recommended Implementations

- Any database middleware packages should support the ANSI SQL query language standard. Microsoft's Open Database Connectivity (ODBC) is a de facto standard for vendor-independent database access and should also be supported.

- IBM, Oracle, Sybase, Informix and Microsoft all have either middleware applications that talk to their database servers or direct web access to their database servers. There are also a large number of third-party middleware applications that interface to database servers from multiple vendors.
- There are no standards that are applicable to web search engines.
- There are no standards that are applicable to text search engines.

Implementation Concerns

- Internet or Intranet search engines are not particularly intelligent. If you don't tell them what your site is about they will just grab your site's home page and characterize your site based on that. If you want to control how your site is profiled you can use "meta" tags on your sites home page html document. For example the two meta entries:
  <META name="description" content="CINCPAC J-3 Home Page">

  <META name="keywords" content="CINCPAC, joint, planning, operations">

  tell the web search engines that your page should be described as the "CINCPAC J-3 Home Page" and that it has to do with CINCPAC's joint planning and operations (those will be the keywords that a user's search will hit on).

- Avoid storing content in a non-indexable format (i.e. PDF)[10].
- Providing explicit notification to index engines to ensure proper or desired information is conveyed to the network public
- If you have a web server that you don't want to have show up in the web search engines or parts of the web site that you don't want indexed, you can create a "robots.txt" file that most of the search engines web crawler robots will respect. The format looks like this:
  #Sample anti-robot file

  User-agent: *

  Disallow: /

  To prevent all indexing

  #Sample anti-robot file

  User-agent: *

  Disallow: /temp

  Disallow:/test

- To prevent indexing of files in the "temp" and "test" directories of your site.

6.7.5 Data Push

A user with a web browser is engaging in a data pull activity, he or she is actively selecting sites and pages of interest and manually navigating to those pages to review the information there. An

[10] PDF, however, makes large volumes of information very portable. This portability versus PDF's inherent lack of "indexability" should be weighed. Often it is little additional effort to create both an HTML and PDF version of a document to achieve both indexability and portability.

alternate mode of information transfer that can be implemented using web technologies is data push. In a data push mode of operation the user has a choice of broadcast channels to choose from and subscribe to. During the subscription process the user decides how often they want the information updated and how the information is to be displayed. Information display can range from small scrolling marquee windows on the desktop, to traditional web browser pages, to dynamic screen savers.

There are currently three popular data push solutions that users may have experience with - PointCast, Netscape's Netcaster, Microsoft's Active Channels. Each of these solutions uses a different technology and is incompatible with the others. The typical use for these push products has been to deliver news and entertainment information from traditional sources (major network news organizations and magazines) to the desktop. The more interesting application for Navy and Marine Corps use is using data push as a way to deliver intelligence updates, morning briefs, general interest administrative material or critical real-time data or alerts. Each of the major commercial push solutions has a "push server" technology that can be adopted by an organization to deliver its own channelized information.

Recommended Implementations

There are currently no standards to govern push technology. Some solutions deliver information in straight HTML format, so the normal web browser and web server standards apply. Microsoft has proposed a new standard - the Content Definition Format (CDF) - for delivery of push data, but no standard body has adopted this proposed standard.

The World Wide Web Consortium (W3C) has released the first public working draft of Synchronized Multimedia Integration Language (SMIL). SMIL is a language that enables authors to bring television-like audio-video content to the Web over low-bandwidth connections. SMIL has the potential to make it easy to produce channels of push content that are much more dynamic than the current text and image pages typically delivered.

Guidelines

Because pushed information is downloaded to the user's system, potentially with frequent updates whether the user is there and reading it or not, pushed information can consume excessive network bandwidth. Organizations can control bandwidth utilization by restricting the number of push channels that are available and implementing local intermediate servers that cache the updates for all the channels instead of downloading the data directly to the user's desktop. Unfortunately, not all push deliver technologies support either of these techniques.

There is momentum behind Microsoft's CDF proposal. However, to use CDF, you have to insert a separate stream of text into your document, in a block of XML (extensible markup language) instead of HTML. That means that each hyperlink on your page has to be coded twice — once in HTML for Web browsers, and again in XML for push clients. XML is the proposed successor to HTML and someday this parallel data format issue will probably go away. In addition, the site designer has to create a separate, master CDF file that contains additional information about the site.

6.8 Network News Service

Internet/Intranet news is the most basic form of smart data pull. The user has a "net news" client program that connects to a "news server". The user then selects "newsgroups" to subscribe to and the client interface shows the active messages in each subscribed to newsgroup and allows the user to retrieve and read the contents of any news "posting" or message. Network News Transfer Protocol (NNTP) specifies the language for communication between the local news server and news clients. NNTP also specifies the language for communication between news servers.

Network news provides a more efficient alternative to e-mail mailing lists. News implementations allow users to pull only the information they are interested in when they are interested in it. News implementations also eliminate the workload of maintaining mailing lists.

The NNTP standard was defined in 1986, and it has stood the test of time very well. NNTP is an open protocol that does not restrict the content of news messages so it has allowed for the evolution of news content from plain text to richer data formats including binary data (typically pictures) and HTML. Support for news content beyond plain text is dependent on the user's client news reader software and the client capabilities of the intended audience must be considered before employing any rich data formats.

There are desirable features for a network news implementation that were not included in the original NNTP standard. These additional features have been added to the basic NNTP functionality by specific vendors. These add-on features include the ability to perform a text search across multiple newsgroups on the server and user-level access restrictions. While useful, these features do not comply with the standard and should generally be avoided.

Best Practices

Use NNTP for network news service. Use network news as the primary means of posting and dialog of information to groups, particularly if the information is not urgent. It can be particularly useful to offload “unofficial” messages of general interest such as bake sales and car washes from the e-mail system. It is also useful, however, to communicate and urgent and important information on a continuing basis to a large number of subscribers on a broadcast or dialog basis.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	NNTP	NNTP	NNTP	NNTP	
Activities, Platforms, Operational Environments		All			

Table 6-12. Network News Standard

The NNTP standard is defined in Request for Comment (RFC) 977 titled Network News Transfer Protocol and dated February, 1986. The introductory paragraph describes NNTP as "a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the Internet community. NNTP is designed so that news articles are stored in a central database allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided."

NNTP 1.5 is the "reference" implementation of the NNTP protocol, but there are many other valid implementations of NNTP compliant news servers and clients available as either free or commercial software.

6.9 References

6.9.1 Standards and Specifications Resources

Domain Name System (DNS)

The DNS provides the service of translating between host names and IP addresses. DNS uses TCP/UDP as a transport service when used in conjunction with other services. See IAB Standard 13, as profiled by MIL-STD-2045-17505

Department of Defense (DOD) MIL-STD-2045-17505: “Information Technology DOD Standardized Profile Internet Domain Name System (DNS);” 29 July 1994; http://www-library.itsi.disa.mil/org/mil_std/ms2045_17505.html (24 May 1998)

Mockapetris (USC ISI); “Domain Names – Implementation And Specification”; (RFC 1035); November 1987; ftp://ftp.isi.edu/in-notes/rfc1035.txt (24 May 1998)

The Open Group (TOG); XFN Specification: “Federated Naming;” July 1995; http://www.opengroup.org/publications/catalog/c403.htm (24 May 1998)
Lottor (SRI Intl.); “Domain Names – Concepts and Facilities” (RFC 1033); November 1987; ftp://ftp.isi.edu/in-notes/rfc1033.txt (24 May 1998)

Directory Services

International Telecommunications Union (ITU) X.500 provides directory services that may be used by users or host applications to locate other users and resources on the network. X.500 also provides security services used by DMS-compliant X.400 implementations.

Kille (Isode Ltd.), Wahl (Critical Angle Inc.), Grimstad, Huber, Sataluri (AT&T); “Using Domains in LDAP/X.500 Distinguished Names” (RFC 2247); January 1998; ftp://ftp.isi.edu/in-notes/rfc2247.txt (24 May 1998)

Electronic Messaging

Hardcastle-Kille (University College London); “Mapping between X.400(1988) / ISO 10021 and RFC 822” (RFC 1327) [See “Crocker”]; May 1992; ftp://ftp.isi.edu/in-notes/rfc1327.txt (24 May 1998)

Crocker (Univ. of Delaware); “Standard for the Format of ARPA Internet Text Messages:” (RFC 822) 13 August 1982; ftp://ftp.isi.edu/in-notes/rfc822.txt (24 May 1998)

Rose (Performance Systems Intl.); “Post Office Protocol – Version 3” (RFC 1225); May 1991; ftp://ftp.isi.edu/in-notes/rfc1225.txt (24 May 1998)

Crispin (Univ. of Washington); “Distributed Electronic Mail Models In IMAP4” (RFC1733); December 1994; ftp://ftp.isi.edu/in-notes/rfc1733.txt (24 May 1998)

International Telecommunications Union – Telecommunications (ITU-T); X.400/F.400 Standard: “Message Handling: System and Service Overview;” July 1996

The standard for electronic mail is the Defense Messaging System (DMS) X.400-based suite of military messaging standards as defined in Allied Communication Publication (ACP) 123 and ACP 123 U.S. Supplement No. 1. The U.S. Supplement annexes contain standards profiles for the definition of the DMS “Business Class Messaging“ (P772) capability; additional standards definition; and DMS use of the Message Security Protocol (MSP)

Joint Staff; Allied Communication Publication (ACP) 123 and ACP 123 Supplement 1: “Common Messaging Strategy and Procedures”; 1 January 1995; http://dmsweb.crcc.disa.mil/dmspub/ACP123%20Mainbody.htm (24 May 1998)

Betanov; “Introduction to X.400”; December 1992, Artech House, Inc.; Norwood, MA;

File Transfer

Basic file transfer shall be accomplished using File Transfer Protocol (FTP). FTP provides a reliable, file transfer service for text or binary files. FTP uses TCP as a transport service. See IAB Standard 9, as profiled by MIL-STD-2045-17504

Department of Defense (DOD) MIL-STD-2045-17504: “Information Technology DOD Standardized Profile Internet File Transfer Profile for DOD Communications;” 29 July 1994; http://www-library.itsi.disa.mil/org/mil_std/ms2045_17504.html (24 May 1998)

Internet Activities Board (IAB); “Protocol Standard For A NetBIOS Service On A TCP/UDP Transport: Concepts And Methods;” (RFC 1001) March 1987; ftp://ftp.isi.edu/in-notes/rfc1001.txt; (24 May 1998)

Auerbach (Epilog Technology Corp.); “Protocol Standard For A NetBIOS Service On A TCP/UDP Transport: Detailed Specifications; (RFC 1002) March 1987; ftp://ftp.isi.edu/in-notes/rfc1002.txt (23 May 1998)

Jurg (SurfNet); “Requirements for IP Version 4 Routers” (RFC 1684); August 1994; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1684.txt (23 May 1998)

7. Computing Resources

This chapter includes computers and associated operating systems, peripherals and communication devices. The relationship of this chapter with the ITSG is shown in Figure 7-1.

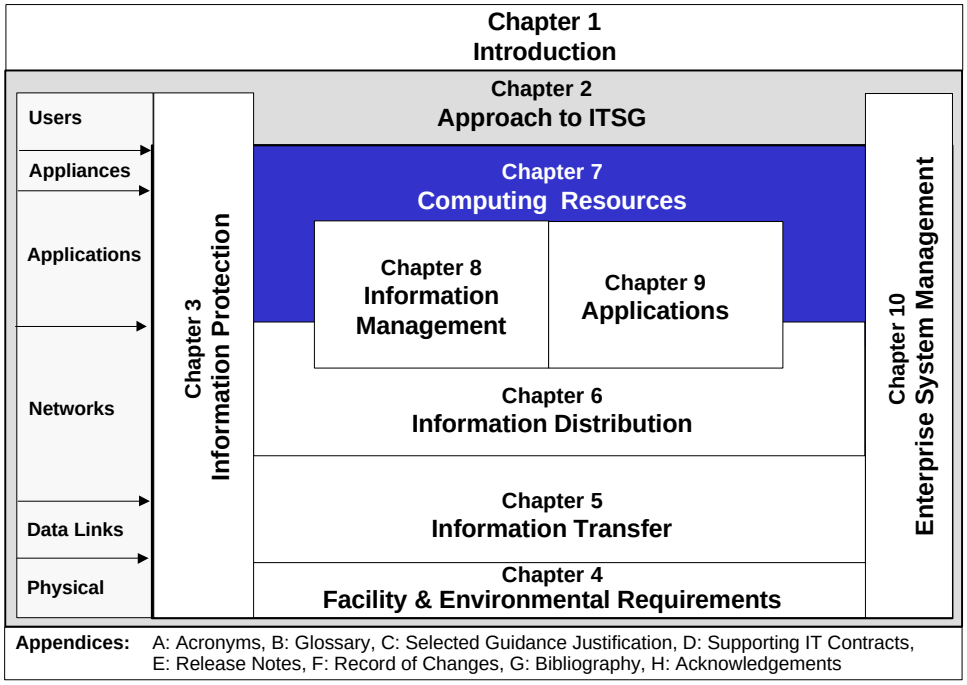


Figure 7-1. ITSG Document Map Highlighting Chapter 7, Computing Resources

7.1 Overview

The purpose of this section is to specify the computing resource standards that the Navy and Marine Corps should use for integrated, interoperable systems that meet the warfighter's minimum information processing requirements. Computing resource standards support the objectives of reducing cost and time of development, easing software integration and maintenance, and improving interoperability. As shown in Figure 7-2, computing resource technology is rooted in, but moves beyond the network technologies represented by the seven layer ISO/OSI model and the previous chapters.

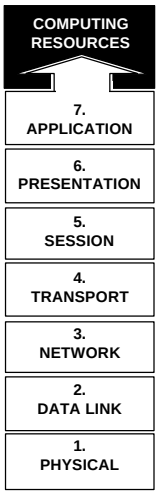


Figure 7-2. ISO/OSI Model and the Computing Environment

7.1.1 Background

The computing resource represents the user's window to the IT world (Figure 7-3). It encompasses the application servers, data servers and presentation clients that make up the three-tiered application architecture discussed in Chapter 9. Figure 7-3 depicts the network-centric model used in the ITSG in the context of the computer-centric DOD Technical Reference Model (TRM) (Figure 2-17). As shown, computing resources provide the connection between the operator, the network, applications and information.

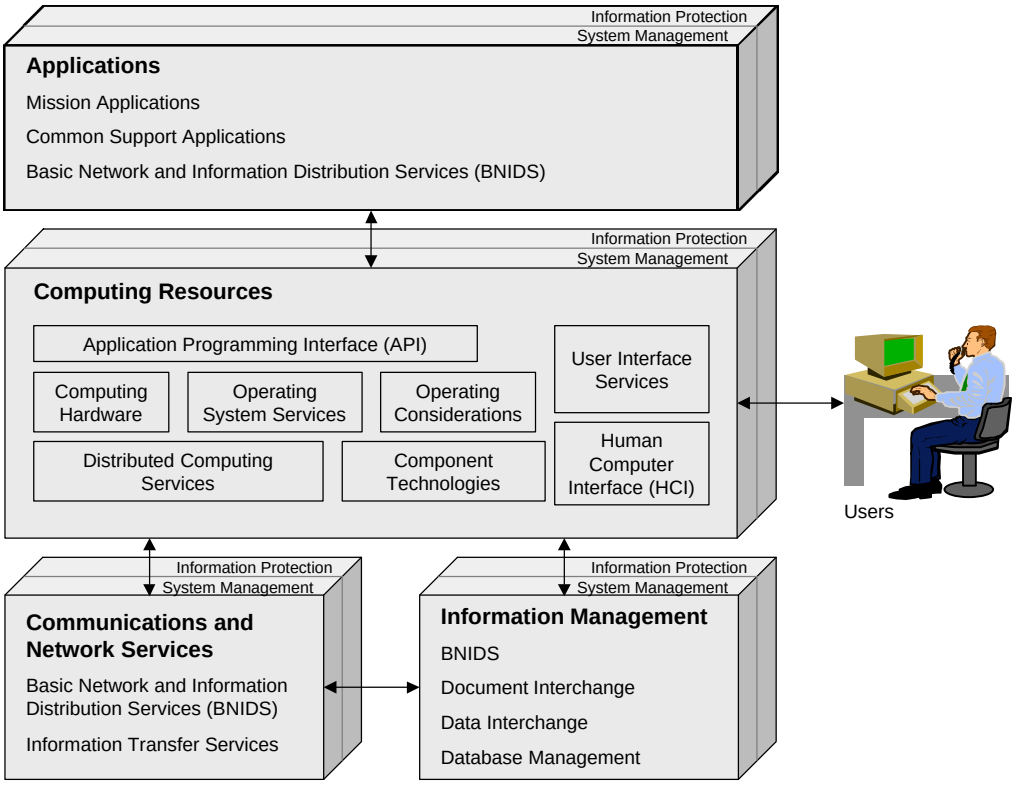


Figure 7-3. Computing Resources in the Context of the DOD Technical Reference Model

7.1.2 Scope of Computing Resources

Computing resources consist of operating system services and computing hardware, and may be based on the considerations of the external environment in which the computing resource is placed. The operating system services consist of an Operating System (OS), Application Programming Interfaces (API) and Human Computer Interface (HCI); they control the system resources in a single machine or distributed environment. The computing hardware includes a Central Processing Unit(s) (CPU), Input and Output (I/O) interfaces, main memory, buses and peripherals. The external environment considerations that affect computing resource selection are security, communications, real-time, and high availability. The computing resource provides the environment necessary to support application software. From the perspective of the application software, services are provided by the computing resource, whether the particular services are provided locally or remotely as part of a distributed system.

7.1.3 General Philosophy

The architecture needed to support a typical application consists of computers that perform as clients and servers. The servers host the primary application software and contain the processing power necessary to support multiple users. Servers also host the data needed to support the application. Figure 7-4 depicts the standard 3-tiered application architecture consisting of (1) an application server, (2) a data server, and (3) presentation clients. Configuration of these elements is more fully discussed in Chapter 9, “Applications.”

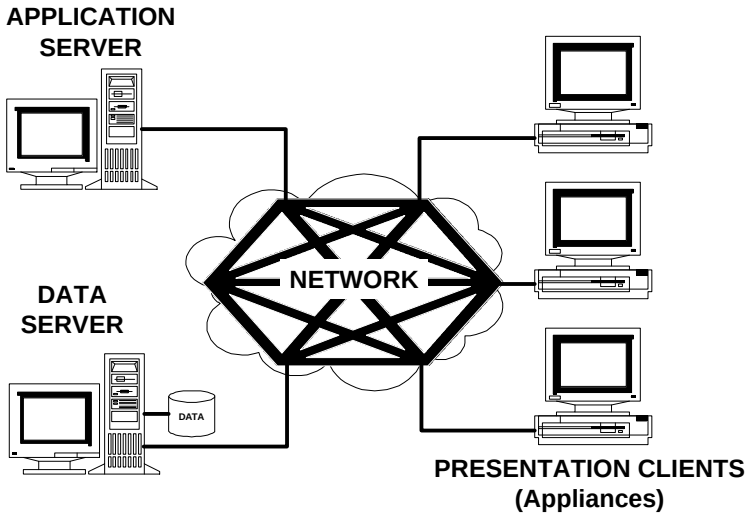


Figure 7-4. Three-Tiered Application Architecture

In the future, almost all application processing software will be hosted on the server computers. The clients will use presentation software that connects to the servers using a common interface[11]. At that time, client computers will likely be less expensive and tailored to the user's individual preference because application interoperability will not be a significant factor. Network computers are an example of personal workstations postured to support this application architecture at lower cost than today's personal computers.

Today, however, most application software is hosted on the client and interoperability among clients is a critical factor. Even within the client-server application architecture, application specific software resident on the client is still prevalent. This demands consistency of client workstations across the entire enterprise to achieve seamless trans-enterprise interoperability, which allows DON business process reengineering. Figure 7-5 outlines the rationale for the DON's client-server enterprise strategy.

Rationale for <u>Heterogeneous Servers</u>

- The server must be tailored to the specific application that may not be supportable by computers most prevalent in the marketplace.
- Many applications work well in their current computing environment and it is not cost effective to change.
- It is not practical to have all applications on a common server for multiple reasons including the need to maintain competition between computer developers and vendors.
- Encourages innovation by not restricting the type of computer used for the development of applications.

[11] Today, the presentation software is a network browser such as Netscape, Internet Explorer, Spry Mosaic, and HotJava.

Rationale for Homogeneous Clients

- Allows for a common, consistent user interface
- Maximizes interoperability
- Minimizes re-training required as users transfer to different organizations within the enterprise.
- Maximizes the ability to use common support and maintenance skills, parts and labor; thereby minimizing cost
- Maximizes portability of support for applications across the enterprise as well as portability of user skills
- Allows for economies of scale in both procurement (volume discounts) and support (more focused skill set for help desk personnel).

State of Application Technology:

- 1999/2000– Client-Server with client-hosted, application-specific software required: Highly dependent on the client's operating system.
- Future – Client-Server without the requirement for application-specific software on the client: dependent on the client's presentation software or network browser. Low dependence on the client's operating system.

Case for Windows NT as Common Client Operating System for 1999/2000

- Member of the Defense Information Infrastructure Common Operating Environment (DII COE)
- Has achieved and is in process of maintaining C2 evaluation criteria for trusted computer systems (Orange Book criteria).
- Supported by a large set of Government Off-The-Shelf (GOTS) software applications such as Defense Message System (DMS), Global Command and Control System (GCCS), Standard Personnel Support System (SPSS), and the Naval Tactical Command Support System (NTCSS)
- Supported by the largest selection of Commercial Off-The-Shelf (GOTS) software applications

Figure 7-5. Rationale for the DON enterprise client-server strategy

Driven by the current state of client-server technology, the general philosophy for implementing computing resources in the DON is the concept of homogeneous clients and heterogeneous servers. Homogeneous clients facilitate providing a consistent interface between the user and the system and make system support and maintenance less complex. Heterogeneous servers support the various computing requirements of applications needed to support DON enterprise missions. The same advantages that homogeneous clients enjoy can be achieved if servers are homogeneous as well. Independent of whether or not the server suite employed is heterogeneous or homogeneous, it is important that they perform their function transparently to the user (i.e., the user neither knows nor cares about the location, number, or vendor of the server being used.) Requiring servers to be homogeneous would restrict the introduction of new server technology which could choke innovation and prevent the enterprise from taking advantage of advances in computing such as massively parallel processors.

Current DON guidance is to develop all new applications such that the client can operate these applications at full capability using a Personal Computer (PC) running Windows NT. An important part of any migration to Windows NT is to identify and assess legacy and high performance computing environments. Many organizations cannot in the near term transfer their applications to Windows NT because of economic or performance issues. The DON CIO will support the connectivity of these legacy and high performance systems to the rest of the Navy and Marine Corps — concurrent with the move to Windows NT. Moreover, the ITSG will support all computing environments needed by Navy and Marine Corps organizations to perform their mission. For example, research and development organizations have a need to continue to expand the frontiers of computer science, and consequently should explore computer technology that offers potential for improving mission capability.

7.2 Computing Hardware

Computing Resources consist of many computing hardware components and configurations of these components. This section covers the various hardware components that make up a computing resource system and examines how these components are commonly configured.

7.2.1 Component Technologies

The major hardware components of Computing Resources are the Central Processing Unit (CPU), one or more backplane buses, main memory (both RAM and cache), Input/Output (I/O) interfaces, and peripherals. This section will examine each of these areas and provide guidance on the selection of these component technologies as part a computing resource system.

7.2.1.1 CPU

The CPU is the “engine” of the computer system and combined with the OS forms the core of the computing resource. Since the OS drives many decisions concerning the computer resource, a CPU that is compatible with the OS becomes an overriding factor in determining the type of CPU. Other than the OS, the main factors to consider in determining the type of CPU for the computer are processing speed (performance) and cost. For computing resources, such as servers and multiprocessors, scalability of the number of processors can be a significant factor in determining CPU.

Best Practices

Choose a CPU that is compatible with the OS of choice, has the performance to meet requirements, and is priced to fit the budget.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Clients & Servers & Special Purpose					
	Pentium II Pentium Pro Pentium AMD K6 Cyrix M2	Pentium II Pentium Pro AMD K6 Cyrix M2	Pentium ? AMD ? Cyrix ?	Pentium ? AMD ? Cyrix ?	Merced
Servers & Special Purpose					
	MIPS Alpha PA-RISC Ultra SPARC Power PC	MIPS Alpha PA-RISC Ultra SPARC Power PC	MIPS Alpha PA-RISC Ultra SPARC Power PC	MIPS Alpha PA-RISC Ultra SPARC Power PC	
Activities, Platforms, Operational Environments		All			

Table 7-1. CPU Recommended Implementations

- The Pentium Pro does not support Multi-Media Extensions (MMX) technology and therefore suffers a performance handicap when compared to the Pentium II, AMD K6 or the Cyrix M2. The Pentium II processor combines the features of the Pentium Pro processor with Intel's MMX technology resulting in the power and speed needed for intensive processing tasks.
- It is recommended that any new Pentium processor support MMX technology. Even on applications that are not graphics/multimedia intensive, there is a 8 – 15 % increase in performance over non-MMX capable PCs.
- Pentium substitutes like AMD K6 and CYRIX M2 are viable and may be considered. The Pentium II can be purchased with SD RAM which speeds up the processor by reducing the wait state from about 60 to 10 nanoseconds.
- The MIPS RISC processor is from the Silicon Graphics, MIPS Group. Alpha is produced by DEC. PA-RISC is from Hewlett-Packard. Ultra Sparc is a Sun Microsystems processor. The PowerPC is from IBM/Motorola. These systems are suitable as servers or special purpose workstations where PCs are not able to perform the required function.

7.2.1.2 Bus

The computer bus connects the different components of the computer resource together and allows them to pass data between them at high speeds. Computer resource configurations, such as COTS personal workstations, often limit or determine the type of bus that will be used. Often there are multiple buses connected together to allow for multiple types of component cards or to extend a non-expandable system bus. Considerations in determining the type of bus to use are: number and type of COTS products compatible with the bus architecture, number of parallel data bit lines, clock speed, and cost. Once the appropriate bus architecture is determined, an important computer resource factor becomes how many interface slots are available on the bus for component cards.

Best Practices

Use buses that provide the necessary performance economically and are compatible with the board level components that are needed to meet requirements. For buses that provide slots for component cards, use standard buses that are supported by multiple vendors providing compatible component cards.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
ISA	PCI	PCI	PCI	PCI	
Microchannel	EISA				
	VME	VME	VME	VME	
	VXI	VXI	VXI	VXI	
	CardBus	CardBus	CardBus	CardBus	
Activities, Platforms, Operational Environments		All			

Table 7-2. Bus Standards

Notes

- Peripheral Connect Interface (PCI) bus is quickly gaining favor as the preferred system bus architecture. PCI provides the necessary throughput to support the high-end data rates required by many of today's applications. Most COTS computers come with a PCI bus.
- EISA bus should be used only to accommodate legacy systems.
- Although VME bus is more popular, VXI bus offers a greater degree of standardization and therefore a greater degree of interoperability between vendor's products. These are the buses of choice for embedded systems.
- CardBus is the new 32-bit high performance bus defined by the new PC Card Standard released by the PCMCIA standards body and trade association. The PC Card Standard replaces the outdated PCMCIA version 2.0 and version 2.1 standards.

7.2.1.3 Main Memory

Main memory is the storage warehouse of the computer where data and programs are stored for efficient processing. In the context of this section, main memory refers to cache and RAM. The main factor to consider in acquisition of a computer system is the quantity (in megabytes) of RAM. Other considerations are access speed, mounting design, and parity. Computer systems with too little memory run slowly, won't load, and crash often. Mounting designs today generally provide for Single In-line Memory Modules (SIMMS) with 72 or 168 pins. The older architecture SIMMS with 30 pins are generally slower and less efficient, and should be avoided to the extent possible.

Cache is usually hard wired to the motherboard and has a faster access time than RAM. Computer system caches of 512 KB or larger are generally satisfactory.

RAM can often be on a separate memory board and is used to store the OS, applications that are running, and data files. The amount of RAM needed for a computer system can vary with the environment and the OS. Servers generally need about an order of magnitude more RAM than personal workstations. For personal workstations with Windows 95, 32MB or more of RAM is recommended; for Windows NT, 64MB or more is recommended. For servers, use the Network Operating System (NOS) guidelines based on the environment. The three major factors used to determine the amount of RAM for a server are number of user connections, number of processes running, and amount of hard drive space.

Best Practices

Acquire enough memory, both cache and RAM, to allow computer performance to meet requirements.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
32 pin RAM FPM	EDO SDRAM DRAM	EDO SDRAM DRAM	EDO SDRAM DRAM	EDO SDRAM DRAM	
Activities, Platforms, Operational Environments		All			

Table 7-3. Memory (RAM) Standards

Notes

While Extended Data Out (EDO) RAM is the current standard for mass market memory, a faster standard emerging is Synchronous DRAM (SDRAM). SDRAM is a memory architecture that incorporates many improvements over traditional DRAM technologies. SDRAM is a new technology that runs at the same clock speed as the microprocessor. The clock on the memory chip is coordinated with the clock of the CPU, so the timing of both the memory and the CPU are "in synch". This reduces or eliminates wait states, and makes SDRAM significantly more efficient than Fast Page Mode (FPM) or even Extended Data Out (EDO) memory.

7.2.1.4 Input/Output (I/O) Interfaces

I/O interfaces allow the computing resource to move data between the “outside world” and the CPU and main memory. Operations like loading a program or file from a floppy or CD, sending and receiving information over the LAN or WAN, or sending a document to the printer to get a hardcopy use I/O interfaces. Quite often the information is sent to or received from a peripheral, which is discussed in the next section.

Best Practices

Use I/O interfaces that use open access standards, support open device connections and are platform independent.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
SCSI-1	SCSI-2	SCSI-2	SCSI-2	SCSI-2	XIO
SSA	SCSI-3	SCSI-3	SCSI-3	SCSI-3	IEEE 1394
Bus & Tag	FC-PH	FC-PH	FC-PH	FC-PH	
IDE	ESCON	ESCON			
	E/IDE				
	IPI	IPI	IPI	IPI	
	PC Card	PC Card	PC Card	PC Card	
	CardBus	CardBus	CardBus	CardBus	
	Serial	Serial	Serial	Serial	
	Parallel	Parallel	Parallel	Parallel	
Activities, Platforms, Operational Environments		All			

Table 7-4. I/O Interface Standards

Notes

- Fibre Channel (FC-PH) is emerging as a host-level interface standard for delivery of high I/O data transfers. FC-PH provides connections for workstation clustering, storage clustering and network-based storage concepts, parallel processing, load leveling, host-to-host or server-to-server communications, host- or server-to-mass storage communications, bulk data transfer, and multimedia. FC-PH is also being used as a system bus at the CPU and memory level as well as a way to cluster multiple systems similar to Non-Uniform Memory Access (NUMA). NUMA describes an architectural approach to clustering multiple systems such that distributed memory appears to the operating system as shared memory. This architectural approach allows a benefit to the user of a shared memory programming model with the scalability of a massively parallel

processor's (MPPs) distributed memory model. FC-PH currently provides up to 1.062 GigaBits Per Second (Gbps) bandwidth using optical fiber.

- FC-PH-based storage subsystems will be supported on mainframes; therefore, the Enterprise Systems Connection or ESCON-based systems will be phased out.
- The Upper Layer Protocol (ULP) over FC-PH from the mainframe will initially deploy as SCSI-2 or SCSI-3 and migrate quickly to Intelligent Peripheral Interface (IPI). IPI will be deployed on large servers before it will be deployed on mainframes. Note that IPI is a protocol only; SCSI is both a protocol and an interface. FC-PH is an interface that can support various ULPs.
- For servers and higher end personal workstations SCSI is the predominant host-level interface for current disk and peripheral devices. As the demand for higher data transfer rates and expanded connectivity requirements increase, SCSI-2 and SCSI-3 over FC-PH in a PCI form factor will be the appropriate long-term direction.
- Enhanced IDE is the predominant peripheral interface for lower end personal workstations. SCSI is the current interface of choice for high-speed devices, such as high-capacity disk and tape drives and is the appropriate long-term direction for both the commodity level and high capacity devices.
- Personal Computer Memory Card International Association (PCMCIA) announced that PCMCIA cards are now referred to as PC Cards. The PC Card Standard defines a 68-pin interface between the peripheral card and the PC Card 'socket' into which it gets inserted. It also defines three standard PC Card sizes, Type I, Type II and Type III. All PC Cards measure the same length and width, roughly the size of a credit card. Where they differ is in their thickness. Type I, the smallest form factor, often used for memory cards, measures 3.3 mm in thickness. Type II, available for those peripherals requiring taller components such as LAN cards and modems, measures 5 mm thick. Type III is the tallest form factor and measures 10.5 mm thick. Type III PC cards can support small rotating disks and other tall components.
- As mentioned under "Bus" (Section 7.2.1.2), CardBus is a new standard introduced as an addendum to the PCMCIA PC Card standard. CardBus is a 32-bit bus mastering card operating at 33 Mhz transferring data at up to 132 MBytes per second. (The 16 bit PC Card bus data rate is 20 MBytes per second.) Like PC Cards, CardBus uses the 68-pin interface but operates at 3.3 volts versus the 5 volts used by PC Cards. CardBus slots are backward compatible with PC Cards. Card sockets can support PC Cards only or CardBus cards only, but not a mixture of the two.
- Serial I/O refers to standard serial interfaces such as RS 232, 422, 423, and 449.
- Parallel I/O refers to standard parallel interfaces such as micro-Centronix
- XIO is an emerging I/O solution based on Specialix' SI controller, and incorporating the high performance I/O processor and communication technology introduced in the RIO range. XIO is ideal for the 16-32 user system where sustaining high performance is essential.
- IEEE 1394, also known as "firewire", is a high speed serial I/O that supports data rates up to 400Mbps

7.2.1.5 Peripherals

Peripherals provide data access, input, storage, and connectivity for a computing resource. The number of peripherals available on the commercial market continues to explode, generally driven by processor speeds, memory/storage capacities and I/O speeds. Although there are many different types of peripherals, such as printers, facsimiles, modems, scanners, video cameras, microphones, speakers, etc., the main issue in specifying/procuring these items is the compatibility of their I/O interfaces with the computer (see Section 7.2.1.4) and application

software. Apart from these compatibility issues, the major considerations for acquiring peripherals are cost and performance (which can include both speed and quality).

A major category of peripherals is static storage devices. As distinguished from main memory (covered in Section 7.2.1.3), static storage devices retain data when the power is off. The remainder of this section will discuss storage devices.

Best Practices

Use peripherals that support standard I/O interfaces and are platform independent.

7.2.1.5.1 Storage Device Standards

Storage refers to the capability to store information outside the central processor. For most computers, the predominant technology for storage has been magnetic disk and will remain so for the next few years.

Storage media is the physical material on which data is stored. The choice of media is usually determined by the application needs in terms of data accessibility, storage density, transfer rates, and reliability. Broad industry standards exist for 3.5″ magnetic disk, 4 mm digital audio tape (DAT), 8 mm helical tape, digital linear tape (DLT), ½″ tape, and compact disk-read only memory (CD-ROM). However, industry is in the process of agreeing on a standard for Digital Versatile Disk (DVD) which will able to read CD-ROMs as well as the new DVDs. Standards do exist for write once read many (WORM) optical and magneto-optical (MO) disks. Although the physical medium for optical technologies conforms to an open standard, the device's recording format may not.

Archived data on outdated storage media (e.g. 5.25" floppy disks) should be transferred to media that is more current to avoid data being "trapped" on obsolete media that cannot be read by devices currently on the market.

As networks proliferate and storage requirements expand, storage technology that uses standard interfaces and promotes hardware and software supplier independence is necessary. This technology will enable us to take advantage of the open systems environment.

Best Practices

Implement storage technology and storage device media that use open access standards, support open device interface standards, and are platform independent.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
5.25″ magnetic disk 5.25″ floppy disk 14″ WORM QIC (quarter inch cartridge) 3420 and 3480 Tape	3.5″ magnetic disk 3.5″ floppy disk 5.25″ and 12″ WORM 5.25″ MO ISO 13346 CD-ROM DVD 8 mm and ½″ helical tape 4 mm DAT DLT Tape 3490E cartridge tape	3.5″ magnetic disk 3.5″ floppy disk 5.25″WORM 5.25″ MO ISO 13346 CD-ROM DVD ½″ helical tape 4 mm DAT DLT Tape 3490E cartridge tape	3.5″ magnetic disk 3.5″ floppy disk 5.25″WORM 5.25″ MO ISO 13346 CD-ROM DVD ½″ helical tape 4 mm DAT DLT Tape 3490E cartridge tape	3.5″ magnetic disk 3.5″ floppy disk 5.25″WORM 5.25″ MO ISO 13346 CD-ROM DVD ½″ helical tape 4 mm DAT DLT Tape 3490E cartridge tape	2.5″ magnetic disk 3.5″ floptical Smart cards High capacity tape Virtual volume tape
Activities, Platforms, Operational Environments		All			

Table 7-5. Storage Device Media

Notes

- 8 mm helical tape is appropriate for backup and archive use; however, it is slow and unreliable for near-line storage solutions where frequent access is required. 4mm DAT offers a faster, more reliable solution to high-capacity and high-access applications.
- ½″ helical tape offers higher storage capacity than 4 mm or 8 mm; however, it is expensive, proprietary, and only Storage Technology supports it.
- 3490E square cartridge ½″ tape is predominantly a mainframe technology for off-line data storage.
- High capacity tape applies capacity multipliers of 2x-4x to current technology. Gains are achieved through increased density factors as well as media length (number of media feet per unit).
- Virtual Volume Tape will exploit tape capacity utilization by building multiple “virtual” tape volumes on a single physical tape media unit; as such, many small and otherwise inefficient tape consumers may be consolidated to achieve nearly 100% utilization of a tape resource.
- Smart cards are being used in Europe and Asia. Smart cards will be used predominantly as an intelligent storage media for providing services to individuals.

- Sony, Phillips, and Toshiba have jointly developed the Digital Video Disk (DVD, also known as Digital Versatile Disk) proposed standard for the CD-ROM industry. The standard allows for dual-sided as well as dual-layered implementations that will increase CD-ROM capacities significantly. In addition, transfer rates may improve to as high as 16 Mega Bits Per Second (Mbps).

7.2.1.5.2 RAID Technology

Redundant Array of Independent Disks (RAID) technology protects from data loss by providing a level of redundancy immediately within an array. The array contains removable disk drive modules that are automatically rebuilt in the event of a device failure without causing the system to shut down. When RAID levels other than 0 are used, no downtime is required to replace a failed disk drive. Data is continuously available while reconstruction of the failed disk occurs in the background.

Much of the benefit of RAID technology lies in its capability to off-load storage management overhead from the host system. To realize this benefit, RAID developers endow their array controllers with significant levels of intelligence. For instance, Adaptive RAID supports multiple RAID levels based on workload characteristics.

Best Practices

Choose the RAID level based on your specific need.

Recommended Implementation

Expiring ITSG	Current ITSG	Projected ITSG			Potential ITSG
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	RAID 1,3,4,5,6 Just a bunch of disks	RAID 1,3,4,5,6	RAID 1,3,4,5,6	RAID 1,3,4,5,6	Adaptive RAID
Activities, Platforms, Operational Environments		All			

Table 7-6. Disk RAID Levels

Notes

For information and guidance for choosing specific RAID levels, see the web page at http://www/cis/ohio-state.edu/hypertext/faq/arch-storage/part1/faq-doc-84.html.

7.2.2 System Configurations

The hardware component technologies mentioned in Section 7.2.1 can be configured in many different ways to accomplish different tasks and meet different requirements. This section examines some of the common configurations (Personal Workstations, Servers, Enterprise Computers and Embedded Computers) with guidance on what component technologies to use for each configuration.

7.2.2.1 Personal Workstation

Personal Workstations (PW) are devices that contain at least one CPU (sometimes several) and provide a user interface, typically a GUI, as well as personal productivity tools, local data storage, and a flexible method for accessing and manipulating data. These PWs are commonly known as Personal Computers or PC's, desktop computers, portables (laptops or notebooks), or workstations and use one of several bus architectures. Low-end PWs are used primarily to support the general office work place. More powerful PWs are predominantly used in high-end compute applications such as Computer-Aided Design/Computer-Aided Manufacturing/Computer-Aided Engineering (CAD/CAM/CAE), application development, multimedia, and decision support data analysis presentation.

Also included in PWs are handheld computers – Personal Digital Assistants (PDAs), also referred to as Personal Information Managers (PIMs). Handhelds are computer systems that fit in a person's hand, and are extremely portable. Handheld systems also tend to have two types of input methods: pen or keyboard. The pen input can be used as digital ink, a mouse, or for handwriting recognition.

Best Practices

Combine components that provide flexible, scaleable, and easy-to-use personal workstations that support the Client/Server model of computing, data access, and multimedia. Allow for an external communication device such as a modem or network interface card.

Recommended Implementation

CPU	Bus	Memory	I/O	Peripherals
Pentium II	PCI	RAM≥64MB	E/IDE	HD>2GB
Pentium Pro		Cache≥512KB		3.5" floppy
Pentium				CD-ROM
AMD K6			SCSI-2,3	
Cyrix M2			PC Card	

Table 7-7. Personal Workstation (Portable) Hardware Configuration Guidance

CPU	Bus	Memory	I/O	Peripherals
Pentium II	PCI	RAM≥64MB	E/IDE	HD>2GB
	EISA	Cache≥512KB		3.5" floppy
				CD-ROM
AMD K6			SCSI-2,3	DVD
Cyrix M2			PC Card or	
			CardBus	

Table 7-8. Personal Workstation (Desktop) Hardware Configuration Guidance

Notes

- EISA bus should be used only to accommodate legacy systems.

Figure 7-6 provides a quick summary of the nominal specifications for Personal Workstation implementation.

	Personal Workstation also used as a Server	**Desktop**	**Laptop**
Processor	Pentium II Pentium Pro Pentium with MMX AMD K6 Cyrix M2 (200MHz Min.)	Pentium II Pentium Pro Pentium with MMX AMD K6 Cyrix M2	Pentium with MMX AMD K6 Cyrix M2
System Bus	PCI	PCI, EISA	PCI
Memory	256 MB SDRAM	64 MB SDRAM	64 MB SDRAM
Input/Output	E/IDE SCSI-3 PC Card X2 Serial Parallel Dual NIC	E/IDE PC Card X2 Serial Parallel Modem NIC (Modem and NIC can be on a PC Card)	E/IDE PC Card X2 Serial Parallel Modem NIC (Modem and NIC can be on a PC Card)
Storage	3.5” Diskette CD-ROM 4mm DAT 9 GB HDD	3.5” Diskette CD-ROM 2 GB HDD	3.5” Diskette CD-ROM 2 GB HDD
Operating System	Windows NT Server	Windows NT Client	Windows 95/98 or Windows NT Client

Figure 7-6. Personal Workstation Configuration Summary

7.2.2.1.1 Network Computers

Network Computers (NCs) are expected to be highly scaleable platforms, spanning a product range from the palmtop to the desktop. They must be attached to a TCP/IP-based network and interoperate with other nodes in the network. Though dependent on the network, NCs may offer some stand-alone functionality.

NCs are not intended to replace personal computers (PCs). Unlike PCs, however, NCs are designed for the network environment. Additionally, NCs are characterized by four specific attributes:

- Architectural neutrality

- Significantly lower total cost of ownership than PCs
- Lower entry price than the typical PC
- Significantly easier use and administration than PCs

In May 1996, Apple, IBM, Oracle Corp., Sun Microsystems, Inc., and Netscape Communications, Inc. announced a set of guidelines for developing low-cost, easy-to-use network computing devices. The NC Reference Profile 1 guidelines provide a common set of standard features and functions across a broad range of scaleable NCs. Architecturally neutral and intended to facilitate the growth of the network computing industry, NC Reference Profile 1 also protects investments made by customers, content providers, system providers, service providers, and application providers through industry-wide compatibility.

Microsoft and Intel have announced the specification for building a competing product to the NC, the NetPC, incorporating management capabilities and operating system features in a sealed PC case. The NetPC is a diskless or disked PC that has no data stored locally; its “identity’’ (user profile and configurations) is server-based.

Best Practices

Much has been said about the NC’s low cost and support benefits; however, these assertions have yet to be proven. Research and development organizations can purchase NCs to investigate potential utility.

7.2.2.2 Servers

Servers are computing resources that can be configured to support groups from small teams (work group servers) to entire sites (campus servers) to geographically dispersed organizations (enterprise servers). Work group servers provide support, such as directory, file, print, and authentication services, in a LAN environment. Campus servers may augment and, for many new applications, replace traditional mainframes. Selecting systems is important that address and support features and services of both systems management and reliability, availability, and serviceability. Campus servers often implement RAID storage technology to provide services with high reliability and availability (see Section 7.2.1.5.2).

There are different types of servers, performing more specific functions. Some of these server types include: database servers, multimedia servers, data push server, applications server, optical disk servers, and mail servers. A brief description of these servers follows:

Database Servers – Large databases make extensive use of disk space and processor power and typically require their own dedicated database server hardware. Increasingly these database servers have more than one CPU and more than one network interface channel to keep up with the demands placed upon them by large numbers of simultaneous users.

Multimedia Servers – If an organization has a large archive of audio or video data, or if it intends to distribute audio or video data in real-time, it will require a multimedia data server. Archives of audio and video data require huge amounts of disk space. Moving this data over the network (typically through streaming audio or video services and protocols) is also resource intensive. Both requirements typically require the dedicated use of a multimedia server.

Data Push Servers – If an organization implements a data push mechanism for distributing information to internal and/or external desktops, it will have to host that push function on a data push server. Depending on the number and volume of channels being pushed, the data push server software may reside on hardware that is also performing other server functionality (typically the web server).

Application Servers – One option for centralizing system management and reducing total cost of ownership in a network environment is to run the actual application programs on a few high-powered application servers rather than on the desktop clients. This is a common approach in UNIX-based computing environments through the use of the X Windows graphical interface to open display and control windows on one system for an application running on another system. A new variation of this approach brings current Microsoft Windows applications to systems that are under powered (old 286 or 386 PCs) or that are not running the Windows95/98 or WindowsNT operating system (UNIX workstations, Java Network Computers). This is made possible by running the applications on shared WindowsNT application servers and just sending the user interface over the network to the user's local system.

Optical Disk Servers – With the huge amounts of reference data available on CD ROM and the increasing availability of CD ROM writers for organizations to use to create their own archival data storage on CD ROM, there is a growing need to have multiple CD ROM disks online at once. A new class of hardware, the CD ROM Server, is a stand-alone network device that includes a large number of CD ROM drives which can be made available as shared disks to all users on a network.

Mail Servers – In an organization that has a number of networked PW clients, mail servers provide store and forward functions for electronic messages. These servers receive, store and distribute electronic messages and require a large amount of storage, proportional to the number of e-mail accounts they carry. They also require numerous network connections and modem connections to receive and distribute messages from/to users and other organizations.

Evaluate servers for their interoperability, portability, reliability, availability, serviceability, and scalability. The capability to easily upgrade processor performance or to add additional processors, disk storage, and communications support extends the life of the platform and enhances the return on investment.

Best Practices

Use hardware components that are standards based, primarily those that are compatible with interface bus standards. Select scaleable servers that can increase performance by adding components and by supporting standards-based network protocols. Through the use of a multiprocessing architecture, hardware should be scaleable and should enable parallel processing.

Recommended Implementation

CPU	Bus	Memory	I/O	Peripherals
Pentium II	PCI	RAM≥256MB*	SCSI-2,3	HD>9GB*
MIPS	VME	Cache≥2MB*		CD-ROM or DVD
Alpha	VXI			RAID 1,3,4,5,6
PowerPC			FC-PH	
PA-RISC			PC Card or CardBus	4mm DAT Tape
Ultra SPARC			IPI	

*Refer to server OS documentation to determine memory requirements

Table 7-9. Server Hardware Configuration Guidance

Notes:

PCI is a system bus architecture and interface standard that will be used to support I/O needs. Unlike SCSI, PCI is not an I/O interface. PCI will likely become the de facto open standard.

7.2.2.3 Enterprise Computers

Large-scale servers and enterprise computers represent the highest level of compute processing capabilities. This group of platforms consists of mainframes, symmetric multiprocessing (SMP) computers, and Massively Parallel Processor (MPP) computers.

Mainframe computers represent a greater share of the large-scale computing environment because they can support numerous terminals and large volumes of batch processing. Mainframes feature mature systems management tools, provide a high-availability operating environment, and support prevalent communications standards. Mainframes also represent an installed base that is entrenched within certain application environments. Within DoD, DISA is consolidating all mainframes into Defense Megacenters to use these expensive resources efficiently. The Standard Operating Environment (SOE) is the standard family of computer hardware and executive software comprising the mainframe operating environments within these Defense Megacenters. The focus of the SOE is on standardizing IBM/IBM compatible and UNISYS mainframe operating environments within the Megacenters.

Symmetric multi-processing (SMP) computers have multiple CPUs, are primarily standards based, and make frequent use of COTS components. SMP computers do not typically scale beyond 16 processors, although 64 processor servers are available. To increase scalability and availability, some SMP suppliers permit multiple computers (all from the same supplier) to be connected by a high-speed link to form what is commonly called a cluster. SMP computers support parallel processing; however, to use this feature, the operating system and the applications must also support parallel processing.

Massively Parallel Processors (MPPs) are generally associated with supercomputers. MPPs can potentially deliver computing power and I/O performance well beyond that of current mainframe and SMP architectures. MPPs promise to deliver high scalability, with some architectures

containing thousands of processors. Typically, however, MPPs are more difficult to program and administer than SMPs.

A convergence is developing between traditional SMP and MPP architectures, resulting in hybrid architectures that borrow technologies from each other. These resulting hybrids show promise in becoming more viable for commercial applications than either of the traditional SMP or MPP architectures.

Best Practices

Avoid proliferation of costly, proprietary mainframe environments. Use open client-server architectures wherever possible. If mainframe environments are the only way to satisfy requirements, conform as much as possible to DISA's SOE.

When possible, avoid proprietary MPP architectures where the operating system and database are nonstandard and not open and where a shared memory programming model is not used.

Use enterprise computers with operating systems and hardware components that comply with IEEE's POSIX and TOG's XPG4 X/Open CAE specifications. Select scaleable servers that can increase performance by adding components and by supporting standards-based network protocols.

Recommended Implementation

CPU	Bus	Memory	I/O	Peripherals
TBD *	TBD *	TBD *	TBD *	TBD *

* To be determined by requirements

Table 7-10. Enterprise Computing Hardware Configuration Guidance

7.2.2.4 Embedded Computers

When COTS computers do not meet the requirements, components must be integrated to form a system. This often involves a design of board level components to perform the necessary functions. The major design consideration is the selection of a back plane bus that will allow all of the components to communicate with each other. This decision can impact dramatically the cost, both in the development and the logistics support of the system. Considerations in determining the bus include availability of Commercial Off-The-Shelf/Government Off-The-Shelf (COTS/GOTS) components and existing systems bus architectures (to reduce the logistics support costs). COTS/GOTS components should be considered first before custom designing and building the components.

Best Practices

When designing embedded computer systems, use industry standard buses and COTS/GOTS components to the maximum extent possible.

Recommended Implementation

CPU	Bus	Memory	I/O	Peripherals
Pentium II	VXI	TBD *	SCSI-2,3	Hard Drive
Power PC	VME		FC-PH	3.5” floppy
MIPS	PCI		IPI	CD-ROM
SPARC			ESCON	DVD
Alpha chip			E/IDE	
			PC Card or CardBus	
			Serial	
			Parallel	

* Varies widely based upon system requirements

Table 7-11. Embedded Computer Systems Hardware Configuration Guidance

Notes:

- Although VME bus is more popular and offers a wider variety of vendor products, VXI bus offers a greater degree of standardization and therefore a greater degree of interoperability among vendors’ products. These are the buses of choice for embedded systems.
- As the popularity of PCI bus rises and the number of COTS products increases, PCI becomes a more desirable architecture for embedded systems.

7.3 Operating System Services

Operating system services consist of the operating system (OS) and the interfaces the OS provides. These interfaces include a Human Computer Interface (HCI) which provides the “look and feel” of the computer system to the user and the Application Programming Interface (API) which provides the “look and feel” of the computer system to applications.

7.3.1 Operating Systems

The operating system (OS) schedules applications and other processes running on the central processing unit (CPU) and controls the exchange of data to and from the computing resource. The OS can reside on a single machine or can operate in a distributed environment. Although the user may not be aware of the single versus distributed environment, the factors to consider in procuring/designing the OS can vary significantly between the two environments. First, in “Local Computing Services” (Section 7.3.1.1), the single computing environment is considered. Next, in “Distributed Computing Services” (Section 7.3.1.2), the distributed computing environment is considered where the span of control of the OS extends beyond the local computing resource to multiple machines.

7.3.1.1 Local computing services

The local computing services are those OS services offered on a single machine. Most commercial OSs fit into this category. Considerations for determining the OS for a single computer environment depend mostly on the applications that will be running on the local machine and the connections needed to communicate with peripherals and the outside world.

7.3.1.1.1 Personal Workstation

As described in Section 7.2.2.2, Personal Workstations (PW) are devices that contain at least one CPU (sometimes several) and provide a user interface, typically a GUI, as well as personal productivity tools, local data storage, and a flexible method for accessing and manipulating data. When purchased off the shelf, PWs will come packaged with an OS. Another OS can be negotiated with the vendor; however, this may mean an added cost.

The major consideration for OS selection is the mix of applications that are intended to run on the PW. Interoperability at the applications level is very important and investigation into each application package is needed to determine the extent of interoperability with other application packages, both on the local PW and within the user's computing community. Another important consideration is communications with other computer resources, although most OSs allow for this. Currently, an important paradigm is the client/server model. Again most OSs allow for this; it is the application software that executes this model. Therefore, the important consideration here is to ensure that the OS is compatible with applications that support the client server model.

NCs support a common Java-based programming environment that enables network-resident applications, as well as stand-alone applications, to be executed on them. The NetPC will run the current Windows OSs (95/98 or NT).

Best Practices

Combine components that provide flexible, scaleable, and easy-to-use personal workstations that support the Client /Server model of computing, data access, and multimedia. Use operating systems that comply with DII COE for long-term usability.

Recommended Implementation

Expiring ITSG	Current ITSG	Projected ITSG			Potential ITSG
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
MS Windows 3.1 and older OS/2 MacOS	Windows NT Workstation Windows 95/98 (non-critical hosts and laptops)	Windows NT Workstation	Windows NT Workstation	Windows NT Workstation	Object-oriented OSs JavaOS Microkernel OSs
Activities, Platforms, Operational Environments		All			

Table 7-12. Personal Workstation Operating Systems

Notes:

- Migration to Windows NT is the appropriate direction in 1999. If business reasons justify a delay in migrating to Windows NT, Windows 95/98 is an acceptable operating system to use through 1999 if currently installed for non-critical systems. Avoid Windows 3.11 and older.
- Sun Microsystems is currently shipping JavaOS.

7.3.1.1.2 Servers

As described in Section 7.2.2.3, servers provide support, such as file, mail, and print services, in a LAN environment. A server's OS is often known as a Network Operating System (NOS).

Major considerations for server OSs are compatibility with client software, network support (at a minimum must support TCP/IP), and server type (applications server, database server, etc.).

World Wide Web (WWW) servers are often supplied as a bundle of hardware, operating systems, and Web-server software. The Web-server software is not an actual operating system; however, Web servers are being used as small to medium sized servers. WWW servers vary in size and complexity, according to the environment where they are deployed.

Best Practices

Use operating systems that comply with DII COE, TOG's X/Open CAE, or the Institute of Electrical and Electronics Engineer's (IEEE's) POSIX specifications. Operating systems should be scaleable, multitasking, multithreaded and enable parallel processing. It is also beneficial if servers are homogeneous with clients. For WWW servers, select products that support a secure version of the HTTP and provide the ability to scale up as volume increases.

Recommended Implementation

Expiring ITSG	Current ITSG	Projected ITSG			Potential ITSG
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
NetWare 3.x or less VINES	Windows NT Server UNIX 95 (X/Open CAE) POSIX NetWare 4.1 or later	Windows NT Server UNIX 95 (X/Open CAE) POSIX NetWare 4.1 or later	Windows NT Server UNIX 95 (X/Open CAE) POSIX NetWare 4.1 or later	Windows NT Server UNIX 95 (X/Open CAE) POSIX	Microkernel OSs
Activities, Platforms, Operational Environments		All			

Table 7-13. Server Operating Systems

Notes:

- SPEC 1170 and the XPG4 specifications are now included within the X/Open CAE specifications.
- Compliance with X/Open CAE and POSIX standards allows for increased interoperability of hardware components and facilitates application portability. Typically the brand, such as X/Open CAE, UNIX 93, and UNIX 95, applies to a combination of platform and operating systems. For example, some Xopen CAE-based, profile-branded platforms include HP-UX 9.X, running on HP 9000 series processors and UnixWare 2.0, the later running on Intel 486 and Pentium platforms.

7.3.1.1.3 Enterprise Computers

As mentioned in Section 7.2.2.4, enterprise computers represent the highest level of computer processing capabilities. Proprietary OSs and custom developed applications are common for these platforms. When determining the OS of enterprise computers, determine the extent to which the applications will need to communicate with other applications or whether the applications will need to run on other systems. If the applications/system will stand-alone and not interact with other systems, then OS should be chosen based on functionality (e.g., development environment, application programming interfaces, scheduling, etc.). If interactions with other systems will occur, ensure the OS is compatible with those systems (e.g., DISA mainframe systems will require compliance with their Standard Operating Environment.).

Best Practices

Use enterprise computers with operating systems that comply with X/Open CAE and IEEE's POSIX specifications. If mainframe environments are the only way to satisfy requirements, conform as much as possible to DISA's SOE.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	X/Open CAE POSIX OS/390 MVS, VM TPF	X/Open CAE POSIX OS/390 VM TPF	X/Open CAE POSIX OS/390 VM TPF	X/Open CAE POSIX OS/390 VM TPF	Microkernel OSs
Activities, Platforms, Operational Environments		Special Purpose Shore Information Producers			

Table 7-14. Enterprise Computer Operating Systems

Notes:

- SPEC 1170 and the XPG4 specifications are now included within the X/Open CAE specifications.
- Product branding for standards such as X/Open CAE, UNIX 93, and UNIX 95 normally applies to a combination of platform and operating systems. For example, some X/Open

CAE-based, profile-branded platforms include HP-UX 9.X, running on HP 9000 series processors.

- Most SMP computers and MPP computers use the UNIX operating system. Two of the major MPP suppliers have proprietary operating systems designed to interface with their own proprietary databases. These proprietary systems have been optimized to address performance issues in specific applications such as large complex queries of large databases.
- MVS and Virtual Machine (VM) are supported when migrating to an open, standards-based platform. Open Edition (Open MVS and Open VME) assists in this migration by providing standards-based tools and capabilities. MVS has been branded recently for base X/Open CAE.
- Transaction Processing Facility (TPF) is an IBM operating system designed to meet the needs of applications that support a large terminal base and require high transaction rates, quick response time, and high availability. TPF continues to improve usability by offering enhanced systems management, ISO-C, TCP/IP, and, eventually, DCE support and POSIX interfaces.
- When system requirements dictate a mainframe solution, use open system technologies whenever possible. Avoid proprietary application support technologies whenever feasible.

7.3.1.2 Distributed Computing Services

Distributed computing services are those application platform technologies that enable a Distributed System Architecture (DSA). A DSA is one in which multiple processing platforms participate cooperatively to accomplish an IM task. Conceptually, DSAs can range in size and scope from a set of dedicated microprocessor systems a few inches apart in an autonomous vehicle to an aggregate of supercomputers spread throughout the country working as a fluid dynamics analyzer. In every case, a protocol is required to enable the individual computers to cooperate. This section currently addresses DSAs connected through standard networks; bus-connected systems are deferred to a future update.

There is no single agreed-upon list of distributed computing services because differing system requirements dictate differing enabling technologies. For example, an application that refers its complex physics analyses to a vector processor may have no need for a time-synchronization service, while an accounting transaction processing system would. To provide guidance, an inclusive but not exhaustive list of services is provided. The services include:

- Remote Procedure Call (RPC)
- Security services
- Directory services
- Time services
- Threads service
- File service
- Object services

The first six services are included in the Distributed Computing Environment (DCE), as defined by TOG. Specifications for open object services have been developed by the Object Management Group (OMG) and are elements of the Common Object Resource Broker Architecture (CORBA).

These standards form the basis for creating heterogeneous distributed applications in both procedure-oriented and object-oriented development environments.

Finally, Inter-Process Communication (IPC) capabilities are required to implement DSAs. In designing a DSA application, candidate IPC technologies should be evaluated carefully for capability, performance, cost, and portability.

7.3.1.2.1 Remote Procedure Call

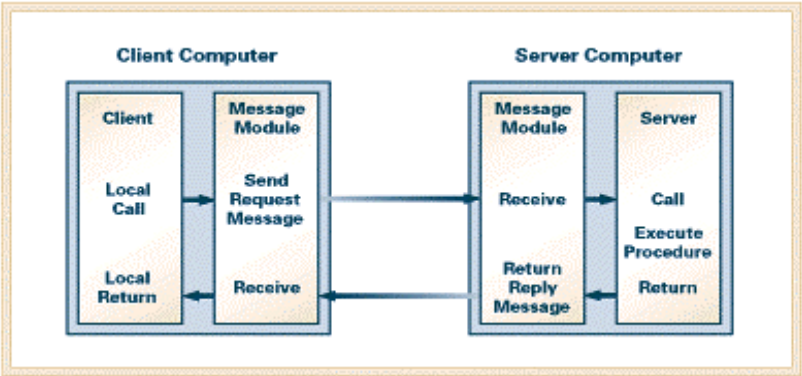


Figure 7-7. Remote Procedure Call

Remote procedure call (RPC) supports DSA designs by enabling a local program to execute procedures located on other computers in the network (Figure 7-7). The local program invokes remote procedures in much the same way as local procedures. Parameter passing between the local and remote procedures is supported. The local program does not need to know the location of the remote procedure; this information is acquired through directory services.

RPC technology can simplify the conversion of an existing monolithic application to a client/server design. To minimize the need for changes to source code, RPC tools can employ a precompiler utility to process Interface Definition Language (IDL) statements, which generate the source code that ensures compatibility between the client and the server.

Best Practices

Use DCE RPC and TxRPC as they become available. If DCE RPC is inappropriate for a specific implementation, use Open Network Computing (ONC) RPC or Netwise RPC.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DCE RPC TxRPC ONC RPC TransAccess RPC	DCE RPC TxRPC ONC RPC TransAccess RPC	DCE RPC TxRPC ONC RPC TransAccess RPC	DCE RPC TxRPC ONC RPC TransAccess RPC	ISO RPC 10148
Activities, Platforms, Operational Environments		All			

Table 7-15. Remote Procedure Call

Notes:

- The DCE RPC, developed by TOG, has been adopted as an Open Group Common Application Environment standard and is the basis for the RPC standard being developed by ISO. The close integration the DCE RPC and the remaining DCE services makes DCE RPC more capable than other RPC technologies.
- TxRPC is a TOG standard that extends the DCE RPC to support transactional semantics for use in a distributed transaction processing (DTP) environment.
- ONC RPC, an older de facto RPC standard developed by Sun Microsystems, Inc., is UNIX-based and uses Transmission Control Protocol/Internet Protocol (TCP/IP). This RPC is simpler in design and more mature than DCE RPC. ONC RPC does not include the sophisticated distributed services that are integrated with DCE RPC.
- The TransAccess RPC, now owned by Proginet, is a mature but proprietary product based upon ONC RPC. Netwise extends the ONC RPC to support both Systems Network Architecture (SNA) logical unit (LU) 6.2 and NetWare Internetwork Packet Exchange/Sequenced Packet Exchange transport protocols. Netwise RPC enables Customer Information Control System (CICS), Information Management System (IMS), time share option, batch, and NetView programs on a Multiple Virtual Storage (MVS) platform to exchange data with RPC programs on other platforms.
- ISO RPC 10148 is an emerging standard.

7.3.1.2.2 Security Services

Security services authenticate the identities of users, authorize controlled access to distributed resources, and provide user and server account management. Security facilities are described fully in Chapter 3.

7.3.1.2.3 Directory Services

Directory services are used to locate distributed resources that reside on a network. Details regarding directory services can be found in Chapter 6.

7.3.1.2.4 Time Services

As stated in Section 6.6.1, time services are established to ensure consistency and accuracy of time and dates across distributed systems. Details regarding time services can be found in that section.

7.3.1.2.5 Threads Service

Threads are independent program elements that, taken together, accomplish the overall program objective. A threaded application can make effective use of a multi-processor computer because different threads can operate simultaneously on different processors. Assigning threads to processors is a function of the operating system. In a DSA, separate networked computers can work together as a larger multi-processor system. Threads service provides an operating-system-like capability to utilize this kind of concurrency in a DSA design.

Best Practices

Use DCE to acquire threads service. Each service implemented in DCE is internally integrated with threads service, giving the designer networked concurrency capability without including it as an application program element.

7.3.1.2.6 File Service

File service provides controlled access to files across a network. File service makes a variety of design options feasible, ranging from NCs and diskless personal workstations to geographically distributed databases.

Different file service products seldom interoperate. Since different file services have been available from different vendors for some time it is likely that incompatible legacy products are now in use. Further, file service products tend to be bundled with operating systems and network operating systems. Establishing a common file service in a heterogeneous DSA environment often requires adding new file service software to at least some systems that already incorporate another file service.

File services use network transport protocols to move data between local and remote computers. Network transport protocols have different characteristics that are inherited by services built upon them. For example, Network File Service (NFS) was originally designed to use User Datagram Protocol (UDP), a low-overhead but unreliable IP-based protocol that made NFS better suited to local-area rather than wide-area networks. NFS on TCP/IP provides greater data integrity in unreliable networking situations.

Access controls and data protection associated with different file service products vary widely. Some products may require add-on user identity services; some transfer clear data (text or binary) across networks. Other products integrate user authentication and encryption options with the basic file service capability.

Best Practices

Use DCE Distributed File Service (DFS).

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DCE DFS	DCE DFS	DCE DFS	DCE DFS	
Activities, Platforms, Operational Environments		All			

Table 7-16. File Service

Notes:

- Avoid file services that are specific to a particular operating system or network operating system.

7.3.1.2.7 Object Services

Object service provides capabilities similar to DCE using an object-oriented paradigm. The primary object service is called an Object Resource Broker (ORB). ORBs are middleware products used to implement object-oriented DSAs. In an ORB environment, a program will invoke a class method belonging to a particular object. The ORB receives the request, resolves it, and returns the results to the invoking program. To resolve the request, the ORB must locate an object supporting the method, invoke it, pass the necessary parameters to the method, and receive the results. The application program doesn't need to know the location of, nor accommodate communication with, any external object; objects can be locally implemented or reside on remote networked computers.

The predominant organization in developing ORB standards has been the Open Management Group (OMG). The Common Object Resource Broker Architecture (CORBA) is the underlying standard for several different commercially-available ORB implementations. OMG's Internet InterORB Protocol (IIOP) is used to assure interoperability among CORBA implementations.

Microsoft Distributed interNet Architecture (DNA) has been proposed as an alternative to the CORBA track. DNA includes the Distributed Component Object Model (DCOM), ActiveX, Active Directories, and several other elements. At present, DNA includes proprietary Microsoft products, limiting its portability.

Best Practices

Choose an appropriate CORBA implementation. Avoid proprietary ORBs that limit portability and opportunities for heterogeneity.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	CORBA 2.1	CORBA	CORBA	CORBA	OMG-submitted ISO
Activities, Platforms, Operational Environments		All			

Table 7-17. Object Service

Notes:

- Commercial CORBA implementations with demonstrated IIOP functionality are available from Digital Equipment Corporation, DNS Technologies, Expersoft, Fujitsu, Hewlett-Packard, IBM, ICL, IONA, Siemens Nixdorf, SunSoft, Tandem, and Visigenic.
- Other compliant products are likely to become available.

7.3.1.2.8 Inter-Process Communication

Inter-Process Communication (IPC) enables the exchange of data between application programs, procedures, or objects. Using IPC technology, programs can exchange data within a single computer or between computers over a network. Each IPC technology provides an API. The two types of IPC technologies are transport dependent and transport independent.

Transport-dependent IPC technologies are generally based on a single transport protocol or operating platform, providing a low-level API that has transport-dependent syntax. These characteristics inhibit application portability. Avoid transport-dependent IPC technologies when possible. Examples of transport-dependent IPCs are Microsoft’s Named Pipes, Novell’s transport layer interface, and IBM’s advanced program-to-program communication (APPC) and Common Programming Interface-Communication (CPI-C).

Transport-independent IPC technologies generally operate independent of transport protocols and operating platforms. These technologies provide a high-level API that has transport-independent syntax, is easy to use, and enables application portability. These technologies include RPC and ORB, above, and interprocess messaging.

Interprocess messaging is a middleware technology that uses message passing and message queuing to provide peer-to-peer asynchronous communication between programs. Messaging is a relatively mature technology that has been widely used for distributed applications involving high transaction rates in the banking, stock market, and airline industries. Few standards exist, however, for portable messaging APIs or interoperable messaging protocols.

7.3.1.2.8.1 Message Passing

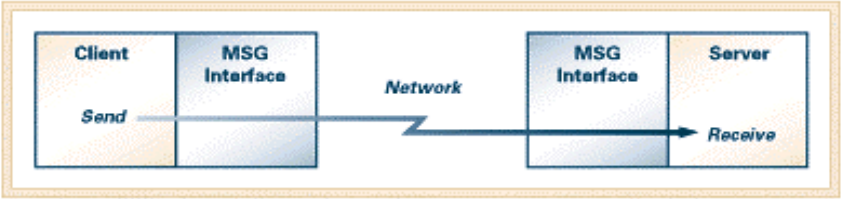


Figure 7-8. Message Passing

The foundation of messaging technology is a message-passing model in which local application programs call an API that can have as few as four verbs: open connection, send, receive, and close connection (Figure 7-8). In a client/server message-passing model, a client sends a request to the server in the form of a message. The server receives the message and processes the request. The server often creates a new message containing the reply and sends this reply message to the client.

Best Practices

Use standards-based products as they become available. Avoid transport-dependent products.

7.3.1.2.8.2 Message Queuing

In many implementations of messaging middleware, the basic message-passing model is enhanced with a message queue to provide a buffer for storing messages that have been sent and are waiting to be acted upon. In this enhanced model, the send verb of the API becomes a put-on-queue operation, and the receive verb becomes a get-from-queue operation (Figure 7-9).

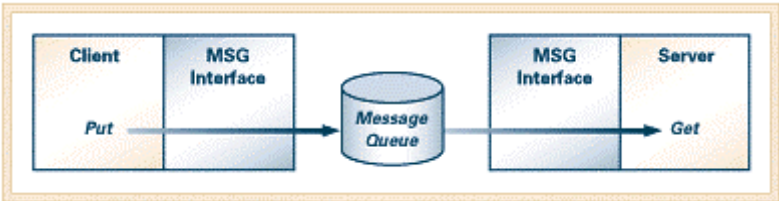


Figure 7-9. Message Queuing

In contrast to other IPC technologies, message queuing is inherently connectionless. In many message-queuing implementations, no direct connection is ever established between the application client and application server. With message queuing, the sender and receiver do not need to be simultaneously available to communicate, nor does the network need to be available directly between the sender and receiver. This capability to support discontinuous communication makes message queuing more tolerant of unreliable networks than other IPC technologies.

Message queuing has other characteristics that can be advantageous in specific application environments:

- Senders and receivers are not required to know each other.
- Messages can be processed in different sequences.
- Persistent queues can guarantee message delivery.

- Shared queues can support load balancing or parallel processing.

A proposed ISO draft standard defines a model, an application layer service definition, and a protocol specification for message queuing. If adopted, this ISO standard may promote interoperability between message-queuing products.

A proposed TOG draft standard defines a message-queuing API. If adopted, this TOG standard may promote source code portability between message-queuing products.

Best Practices

Use standards-based products as they become available. Avoid transport-dependent products.

7.3.2 Application Programming Interface

The OS or a shell on top of the OS will provide an interface by which application programs can exchange information with and access the computing resource. This interface, called the Application Programming Interface (API), defines the services that are available to applications. Having a common API across systems or organizations will promote the portability of application software written for that API. Commercial OSs (e.g. Windows NT) have an API that commercial application vendors build to. If a system is not used for application development, APIs are of little consideration in the procurement of a computing resource. The main consideration for those systems is the interoperability of the data among various applications (e.g., can a Word file be read and edited by a WordPerfect application?)

A key component of the DON application systems architecture will be a set of platform-independent APIs. Application platform differences will be “masked” by software for functional compensation and API translation. As application software is ported to new environments, high-level APIs and software to compensate for differences in the underlying products must be provided. To address these issues, the application systems architecture must supply design guidelines and APIs that will provide the required level of portability with minimum effort. An example of this is the migration of the Joint Maritime Command Information System (JMCIS) from UNIX to Windows NT.

Three dimensional (3D) graphics applications are becoming popular because they provide a more realistic representation of an information space and contribute to the development and maintenance of situation awareness by the warfighter. Because of 3D applications’ reliance on hardware and software architectures to support numerically intensive calculations and the rapid changes in these architectures, standards for 3D APIs are in a state of development by several organizations. The APIs for 3D computer graphics can be divided into those targeted toward the engineering and business requirements and those that support the video game environment. The 3D API for video games is a competitive environment with many players and few people willing to risk supporting a single API.

The APIs for the engineering and business environment are more mature. PHIGS, OpenGL, and HOOPS are currently competing in this market. Other 3D APIs (such as Open Inventor) exist in this market, but they tend to support slightly different goals.

Best Practices

The computing resource services should be accessed by applications through either the standard Win32 APIs, Portable Operating System Interface (POSIX), or TOG Single UNIX specification, version 2. Not all computing resource services are required to be implemented, but those that are used shall comply with the standards listed below.

The following standards are recommended:

- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993 or later, Microsoft Press.
- ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Application Program Interface (API)[C language] (The C Language is part of the formal title of this standard. It denotes the language used to define the standard.) (Mandated Services)
- ISO/IEC 9945-1: 1996:(Real-time Extensions)
- ISO/IEC 9945-1: 1996: (Threads Extensions)
- ISO 9945-2: 1993, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 2: Shell and Utilities, (as profiled by FIPS PUB 189: 1994)
- IEEE 1003.2d: 1994, POSIX - Part 2: Shell and Utilities - Amendment: Batch Environment
- IEEE 1003.5 - 1992, IEEE Standard for Information Technology - POSIX Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API)
- IEEE 1003.5b - 1996, IEEE Standard for Information Technology - POSIX Ada Language Interfaces - Part 1: Binding for System Application Programming Interface (API) - AMENDMENT 1: Real-time Extensions
- Single UNIX Specification, Version 2, API, The Open Group

7.3.3 Human Computer Interface

The Human Computer Interface (HCI) refers to the way a user interacts with a computer, including the display and manipulation of information as well as the user's method of input and navigation within a system. HCIs are not limited to a visual display of information on a screen. Selection and use of I/O devices, such as the mouse, touch screen, and data glove, are considerations in the design of an effective HCI.

7.3.3.1 HCI Style Guides

An HCI style guide is a document that specifies design rules and guidelines for the look and behavior of the user interaction with a software application or a family of software applications. The style guide represents "what" user interfaces should do in terms of appearance and behavior, and can be used to derive HCI design specifications which define "how" the rules are implemented in the HCI application code.

Figure 7-10 illustrates the hierarchy of style guides to maintain consistency and good HCI design within the DON. This hierarchy, when applied according to the process in the DoD HCI Style Guide, provides a framework that supports iterative prototype-based HCI development. The process starts with top-level general guidance and uses prototyping activities to develop system-specific design rules.

The interface developer shall use the selected commercial GUI style guide, refinements provided in the DoD HCI Style Guide, and the appropriate domain-level style guide for specific style decisions along with input of human factors specialists to create the system-specific HCI.

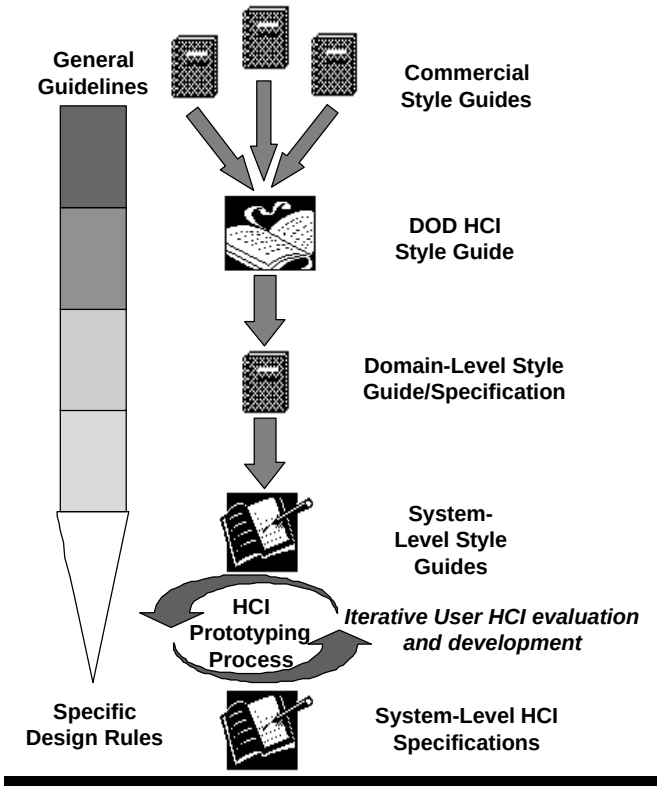


Figure 7-10. HCI Development Guidance

Most Web-based interfaces use Hypertext Markup Language (HTML) to describe the structure of the information they contain. The next version of the DoD HCI Style Guide and the User Interface Specifications for the Defense Information Infrastructure (DII) are expected to address HTML-based interfaces. The next version of the user interface specification for the DII addresses MS Windows based interfaces.

7.3.3.2 HCI Development

For many systems, COTS products will be used exclusively and there will be no development of an HCI. For some other systems, applications will be developed for a commercial OS, but there will also be no development of an HCI. Rather the HCI that is part of the OS will be used and will be quite satisfactory. Still other systems may have no HCI at all but rather get input from sensors and provide outputs to controller devices. For the remaining systems, special requirements will necessitate the development of an HCI.

This section provides guidance for HCI development and implementation in DON automated systems. The objective is to standardize user interface design and implementation options thus enabling DON applications within a given domain to appear and behave consistently. The standardization of HCI appearance and behavior within the DON will result in higher productivity, shorter training time, and reduced development, operation, and support costs. The following sections include specific guidance regarding the style guide hierarchy levels.

7.3.3.2.1 Character Based HCIs

For all DON automated systems, the near-term goal is to convert character-based interfaces to GUIs. Although GUIs are the preferred user interface, some specialized devices may require use of character-based interfaces due to operational, technical, or physical constraints. These specialized interfaces shall be defined by domain-level style guides and further detailed in system-level user interface specifications. In order to present a consistent interface to the user, application software shall not mix command line user interfaces and GUIs.

Best Practices

The following is mandated for systems with a requirement for a character-based interface:

- DoD HCI Style Guide, TAFIM Version 3.0, Volume 8, 30 April 1996.
- While not mandated, additional guidance for developing character-based interfaces can be found in ESD-TR-86-278, Guidelines for Designing User Interface Software (Smith and Mosier 1986).

7.3.3.2.2 Commercial Style Guides

When developing DON automated systems, the graphical user interface shall be based on one commercial user interface style guide. Hybrid GUIs that mix user interface styles (e.g., Motif with Windows) shall not be created. A hybrid GUI is a GUI that is composed of tool kit components from more than one user interface style.

Best Practices

A commercial GUI style shall be selected as the basis for user interface development.

The following is mandated for a Microsoft Windows-based environment:

- The Windows™ Interface Guidelines for Software Design, Microsoft Press, 1996 (Defines the Windows 95 and Windows NT 4.x HCI).

For UNIX workstations, the style guide corresponding to the selected version of Motif is mandated:

- Open Software Foundation (OSF)/Motif Style Guide, Revision 1.2 (OSF 1992)
- TriTeal Enterprise Desktop (TED) 4.0 Style Guide and Certification Checklist, Carlsbad, CA: TriTeal Corporation, 1995.

7.3.3.2.3 Enterprise-level Style Guides

The DoD HCI Style Guide focuses on elements of user interface design not normally addressed in a commercial style guide and concentrates on DoD-specific functional areas such as display of security classification markings, mapping display and manipulation, decision aids, and embedded training. The DoD Style Guide is intended to provide guidelines on good HCI design, it represents DoD policy and all DoD information systems are required to comply with its provisions.

Best Practices

The following guideline is mandated:

- DoD HCI Style Guide, TAFIM Version 3.0, Volume 8, 30 April 1996.

7.3.3.2.4 Domain-level Style Guides

Domain-level style guides provide detailed guidance that addresses the requirements of a particular domain (e.g., C4ISR) as defined by a DoD organization (e.g., joint, individual service, or agency). Domain-level style guides reflect the consensus of the organization on the look and feel they want to provide in their systems. Over time, it is expected that DoD organizations will develop and publish domain-level style guides for directing the HCI design efforts for their systems. The domain-level style guide is the compliance document for these systems and may be supplemented by a system-level style guide as needed.

Best Practices

The following style guide is mandated for C4ISR and combat support domain systems.

- User Interface Specification for the Defense Information Infrastructure (DII), Version 2.0, June 1996.

7.3.3.2.5 System-level Style Guides

System-level style guides provide the special tailoring of commercial, DoD, and domain-level style guides. These documents include explicit design guidance and rules for the system, while maintaining the appearance and behavior provided in the domain-level style guide. If needed, the Motif-based system-level style guide will be created in accordance with the User Interface Specification for the DII.

7.3.3.3 Symbology

The following standard is mandated for the display of common warfighting symbology:

- MIL-STD-2525A, Common Warfighting Symbology, 15 December 1996.

7.4 Operating Considerations

Often there are broad external considerations that effect the design/specification of a computing resource. This section discusses some of these considerations and how they effect the design/specification.

7.4.1 Security

Although security requirements are often considered at the end of a system design or after the system is procured and installed, much time, effort and money can be saved if security is considered first. From the computer resource point of view, security can affect the specification of the OS and some of the hardware (such as removable vs. permanent hard drives or dynamic vs. static memory). A detailed discussion of Security is provided in Chapter 3.

7.5 Communications

Almost all computing resources will require a network connection. Even if it is determined that external communications will not be required immediately, it is wise to accommodate a network

interface card or modem in the computing resource design/specification. Standards play a critical role in this area and compatibility is by far the most important factor to consider. A further discussion of computer communications is provided in Chapter 5, Information Transfer and Chapter 6, Information Distribution.

7.5.1 Real Time

Often, real-time systems are thought of as being fast. The real consideration in a real-time system is meeting a process's deadline. There are hard deadlines where, if missed by the process, the data produced by the process is useless. Then there are soft deadlines where, if missed by the process, the value of the data is degraded. Sometimes these deadlines are based on human perceptions and can vary from person to person. For example, how much delay in a video teleconference is tolerable?

The scheduling of many processes on the CPU and accessing peripherals can be critical in real-time systems. When specifying OSs for systems where significant or catastrophic failures can occur when processes are not scheduled properly, consider very carefully the method by which the OS schedules processes. There should be some means of specifying the priority of processes so that a lower priority process does not prevent a higher priority process from meeting its deadlines and causing potential damage to the system, people or environment. In non real-time systems, other considerations will probably take precedence, such as cost, portability of applications, availability, or network capabilities.

Best Practices

When specifying a computer resource for a real-time system, hardware that operates at higher clock speeds (faster) is more desirable. Also use OSs that comply with ISO/IEC 9945-1: 1996:(Real-time Extensions). When considering real-time distributed systems, also refer to IEEE P1003.21-standard interfaces to real-time distributed communications.

7.5.2 High Availability

Some systems require high availability because of the high cost incurred when these systems are down (e.g. tactical systems or an organizations IT infrastructure). Systems with high availability achieve fault tolerance through redundant, distributed or protected (low vulnerability to attack) methods. High-availability systems are equipped with features that make them reliable and, therefore, fail less often than regular systems. When failure does occur, however, high-availability systems can be restored faster and more accurately than regular systems. Advanced levels of high-availability systems provide even greater capabilities:

Fault-resilient systems (or high-resiliency systems) – These systems have a component of hardware detection at the computing level. Although major elements of the computer can bring down the system or portions of it, minor components can fail without interruption. Failed components—power supplies, system fans, disk drives, and some I/O controllers—can be replaced without service downtime. The fault-resilient system is expected to reduce downtime by 50 percent. The system averages less than five minutes downtimes for recovery if the design and implementation are sound.

Fault-tolerant systems – These systems have redundant hardware components that continually check the other component's integrity. If one component is in error, the system

eliminates that component from the environment and notifies the operator that a failure has occurred. All failed component replacement occurs while the system is running. The component is restored to the environment with no penalty to the application. Recovery is less than one second, and all unplanned downtime is eliminated.

Continuously available systems – These systems are fault-tolerant systems that eliminate all downtime, planned and unplanned. The hardware and software can be upgraded while the system is on-line.

Some features provided by high-availability systems can be furnished through Transaction Processing (TP) monitors and some commercial database systems. Some software must be present to detect a failure and initiate the recovery process. The recovery process involves switching processing to another machine and synchronizing critical data to ensure integrity. Corruption or loss of data is determined before the processing continues. Various levels of sophistication exist, but with sophistication comes complexity and, usually, additional costs.

Some other methods that increase the availability of a system are the use of uninterruptable power supplies, RAID systems (see Section 7.2.1.5.2), systems that allow live insertion of components, distributed systems, multiple path connectivity,

Best Practices

Select system elements and design in redundancy based on the level of tolerance for unplanned downtime. Avoid single points of failure and bottlenecks in the system design. Assemble components commensurate with cost issues, functionality, and associated risk.

7.6 References

7.6.1 Standards and Specifications Resources

Computer I/O Interface Standards

American National Standards Institute (ANSI); ANSI X3.230-1994. Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH). 1994; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.230-1994. Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH). 1994; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.230-1994/AM 1-1996. Information Technology – Fibre Channel Physical and Signaling Interface (FC-PH) – Amendment 1. 1996; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.297-1997. Information Technology – Fibre Channel – Physical and Signalling Interface-2 (FC-PH-2). 1997; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.131-1994 : Information Systems - Small Computer Systems Interface-2 (SCSI-2); 1997; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.253-1995 : Information Technology - SCSI-3 Parallel Interface (SPI); 1995; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.232-1996 : Information Technology - SCSI-2 Common Access Method Transport and SCSI Interface Module; 1996; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.269-1996 : Information Technology - Fibre Channel Protocol for SCSI; 1996; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.270-1996 : Information Technology - SCSI-3 Architecture Model (SAM); 1996; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.277-1996 : Information Technology - SCSI-3 Fast-20; 1996; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.294-1996 : Information Technology - Serial Storage Architecture- SCSI-2 Protocol (SSA-S2P); 1996; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI/AIIM MS58-1996 : Standard Recommended Practice for Implementation of Small Computer Systems Interface (SCSI-2), (X3.131.1994) for Scanners; 1996; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.276-1997 : Information Technology - SCSI-3 Controller Commands (SCC); 1997; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.292-1997 : Information Technology - SCSI-3 Interlocked Protocol (SIP); 1997; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.301-1997 : Information Technology - SCSI-3 Primary Commands (SPC); 1997; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI X3.304-1997 : Information Technology - SCSI-3 Multimedia Commands (MMC); 1997; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI NCITS 309-1997 : Information Technology - Serial Storage Architecture - SCSI-3 Protocol (SSA-S3P); 1997; www.nssn.org (23 May 1998)

American National Standards Institute (ANSI); ANSI NCITS 306-1998 : Information Technology - SCSI-3 Block Commands (SBC); 1998; www.nssn.org (23 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: 1394-1995 “IEEE Standard for a High Performance Serial Bus;” 1985; http://standards.ieee.org/db/status/ (23 May 1998)

Computer Bus Standards

Institute of Electrical and Electronics Engineers (IEEE) standard: 1014-1987 “IEEE Standard for a Versatile Backplane Bus: VMEbus;” 1987; http://standards.ieee.org/db/status/ (23 May 1998);

Institute of Electrical and Electronics Engineers (IEEE) standard: 1155-1992 “IEEE Standard VMEbus Extensions for Instrumentation: VXIbus;” http://standards.ieee.org/db/status/ (23 May 1998)

Computer OS Standards

International Organization for Standardization (ISO) standard: ISO/IEC 9945:1996, “Information Technology - Portable Operating System Interface for Computer Environments (POSIX);” 1996; http://www.iso.ch/cate/cat.html (23 May 1998)

The Open Group (TOG), X/Open CAE Specification: “System Interface Definitions, Issue 4, Version 2;” September 1994; http://www.opengroup.org/publications/catalog/c434_a.htm (23 May 1998)

The Open Group (TOG), X/Open CAE Specification: “System Interfaces and Headers, Issue 4, Version 2;” September 1994; http://www.opengroup.org/publications/catalog/c435.htm (23 May 1998)

The Open Group (TOG), X/Open CAE Specification: “Commands and Utilities, Issue 4, Version 2;” September 1994; http://www.opengroup.org/pubs/catalog/c436.htm (23 May 1998)

The Open Group (TOG): “The Single UNIX Specification” - 5 Volume Set for UNIX 95 Open Group Publication Set T910; July 1996; http://www.opengroup.org/pubs/catalog/t910s.htm (23 May 1998)

Distributed Computing Services Standards

The Open Group (TOG): “Distributed Computing Environment (DCE) Version 1.2.2;” 1997; http://www.camb.opengroup.org/tech/dce/ (24 May 1998)

Open Management Group (OMG); “The Common Object Request Broker Architecture (CORBA) and Specification Revision 2.2;”1 February 1998; http://www.omg.org/corba/corbiiop.htm (24 May 1998)

Defense Information Infrastructure Common Operating Environment (DII COE)

Defense Information Systems Agency (DISA); “Defense Information Infrastructure Common Operating Environment (DII COE);” 1 May 1998; http://spider.osfl.disa.mil/dii/ (24 May 1998)

Application Programming Interface (API)

Microsoft Inc.; Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual; 1993, Microsoft Press, Redmond, WA

International Organization for Standardization (ISO) standard: ISO/IEC 9945-1:1996, “Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Application Program Interface (API)[C language];” 1996 ;http://www.iso.ch/cate/d24426.html (24 May 1998)

International Organization for Standardization (ISO) standard: ISO 9945-2: 1993, “Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 2: Shell and Utilities”, (as profiled by FIPS PUB 189: 1994); 1993; http://www.iso.ch/cate/d17841.html (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1003.2d: 1994, “POSIX - Part 2: Shell and Utilities - Amendment: Batch Environment;” 1994 http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1003.5 - 1992, IEEE “Standard for Information Technology - POSIX Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API);” 1992; http://standards.ieee.org/db/status/ (24 May 1998)

Human Computer Interface (HCI)

Defense Information Systems Agency (DISA) Document CM-400-18-04: User Interface Specification for the Defense Information Infrastructure (DII), Version 2.0, June 1996

Department of Defense (DoD): Human Computer Interface (HCI) Style Guide”, TAFIM Version 3.0, Volume 8; 30 April 1996; http://www.library.itsi.disa.mil/org/dod_std/dod_hci_sg_v3_0.html (24 May 1998);

Smith, Mosier (MITRE); “Guidelines for Designing User Interface Software (ESD – TR-86-278)” 1996; http://www.syd.dit.csiro.au/hci/guidelines/sam/gintro.html (24 May 1998)

Open Software Foundation (OSF)/Motif™ Style Guide, Revision 1.2 (OSF 1992)

TriTeal Corporation; TriTeal Enterprise Desktop (TED) 4.0 Style Guide and Certification Checklist, TriTeal Corporation, Carlsbad, CA; 1995

Microsoft Inc.; The Windows™ Interface Guidelines For Software Design, 1996; Microsoft Press; Redmond WA

Tactical Symbology

Department of Defense; MIL-STD-2525A, “Common Warfighting Symbology;” 15 December

Real Time Requirements

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1003.5b - 1996, “IEEE Standard for Information Technology - POSIX Ada Language Interfaces - Part 1: Binding for System Application Programming Interface (API) - AMENDMENT 1: Real-time Extensions;” 1996; http://standards.ieee.org/db/status/ (24 May 1998)

7.6.2 Supporting Resources

Further technical information on the various aspects of the computing resource can be found at the following web sites:

Fiber Channel Association web site: http://www.fibrechannel.com (24 May 1998)

Intel Inc. iCOMP (r) web site: http://www.intel.com/procs/perf/icomp/index.htm (24 May 1998)

Microsoft Inc. web site: http://www.microsoft.com (24 May 998)

National Committee on Information Technology Standards (NCITS) T10 Technical Committee on Lower Layer Interfaces web site: http://www.symbios.com/x3t10/Welcome.html (24 May 1998)

Network Computer Consortium web site: http://www.nc.ihost.com/ (24 May 1998)

Object Management Group (OMG) web site: http://www.omg.org (24 May 1998)

PCI Special Interest Group web site: http://www.pcisig.com (24 May 1998)

Personal Computer Memory Card International Association web site: http://www.pc-card.com/ (24 May 1998)

Personal Digital Assistant (PDA) Industry Association web site: http://www.pdaia.org/ (24 May 1998)

Space and Naval Warfare Systems Command, PMW 171 web site: http://c4iweb.spawar.navy.mil (24 May 1998)

The Open Group Website: http://www.opengroup.org (24 May 1998)

8. Information Management

This chapter addresses DON information policy, information requirements definition, information interchange, database management and interoperability and data metrics. The relationship of this chapter with the ITSG is shown in Figure 8-1.

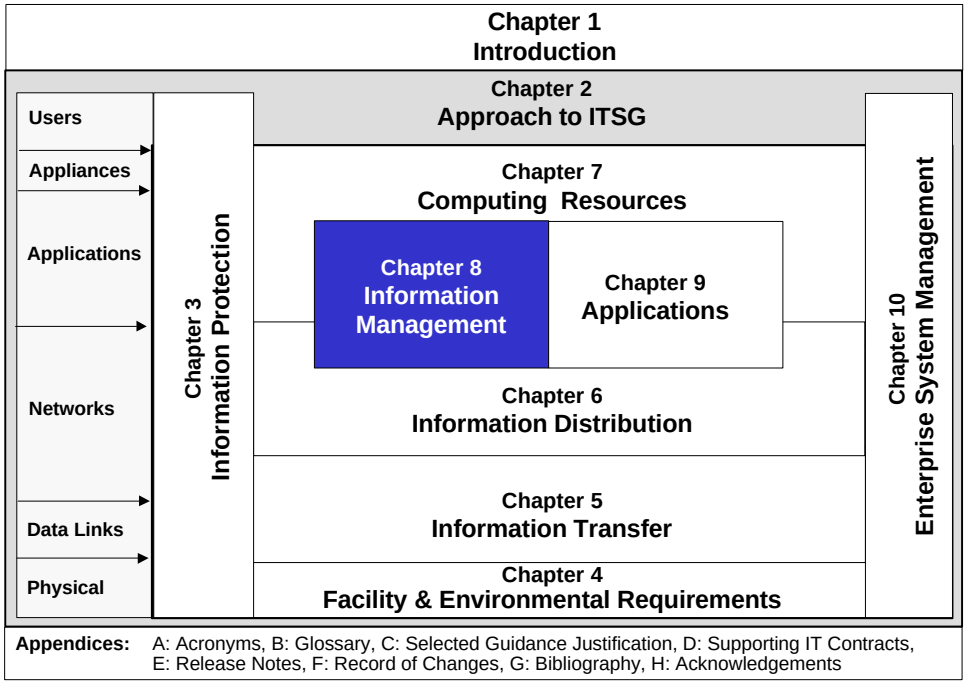


Figure 8-1. ITSG Document Map Highlighting Chapter 8, Information Management

Information is the assembly and presentation of data in a form that is understandable and valuable for conveying knowledge and making decisions. It is the “payload” of the information infrastructure. Information management is critical to the execution of individual Navy and Marine Corps mission functions.

The information challenge in our Navy and Marine Corps operating environments is unparalleled because of required force mobility, unit dispersion, and the multitude of missions. Requirements for the right information at the right time in the correct amount to the right place increase exponentially when the warfighter is placed in a forward area conflict environment. Fleet commanders need and expect high quality information that will enable them to quickly respond to the challenges that confront them. In this environment, information weighs heavily on the outcome and is often a primary determinant of success or failure. This requirement, as stated in Joint Vision 2010, supports information superiority for our warfighters.

Transforming raw data into useful information is the job of information managers (C4ISR, Combat Systems, Logisitics, Personnel, Medical, Acquisition, and Modeling and Simulation). The relationship of information management within the information infrastructure (Facilities, Communications, Hardware, and Software Applications) is shown in Figure 8-2. The capability of today’s information systems can produce outcomes of two potential extremes – totally overwhelm the user with unusable information or deliver critically important information in a timely manner. The objective of information management is to maximize the timely delivery of essential information in a usable structure.

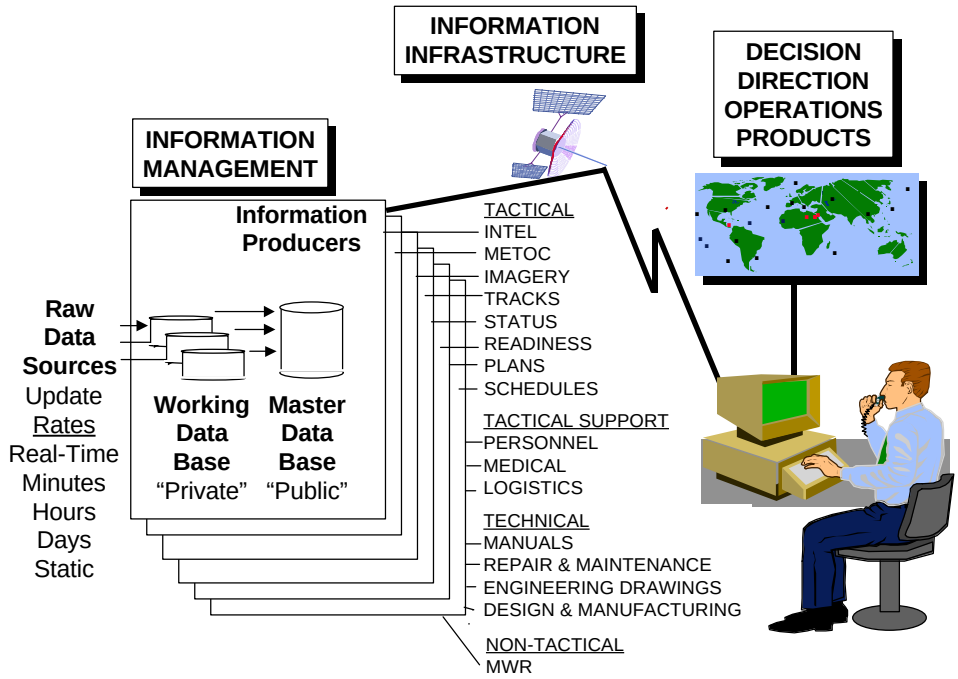


Figure 8-2. Relationship Between Information Management, Information Infrastructure, and Operations

Creating useful information from data involves transformations of the data into multiple media and formats:

- Formatted for transmission over communication links
- Encrypted for security
- Compressed for efficiency
- Structured for storage, retrieval, processing, manipulation and presentation

Each transformation requirement provides an opportunity to stop, delay, attenuate, or corrupt the information. Minimizing the amount of transformations that have to occur is fundamental to providing useful information. Accuracy, precision, and timeliness of information are often best achieved if the information is maintained at the source vice the destination. Operators at the source of the information have a better understanding of the surrounding situation. They, therefore have the greater capability to produce accurate information with higher precision. Today's information technology allows more operators to directly manage the source. This information base can then be shared with remote processors or join with other remote information bases for greatly improved sharing and data interoperability.

This chapter describes the role of information management in the development, maintenance, and implementation of the objective DON enterprise architecture and standards discussed in Chapter 1. The modified DOD Technical Reference Model (TRM) in Figure 8-3 shows that information management involves Basic Network and Information Distribution Services (BNIDS); BNIDS is discussed in Chapter 6.

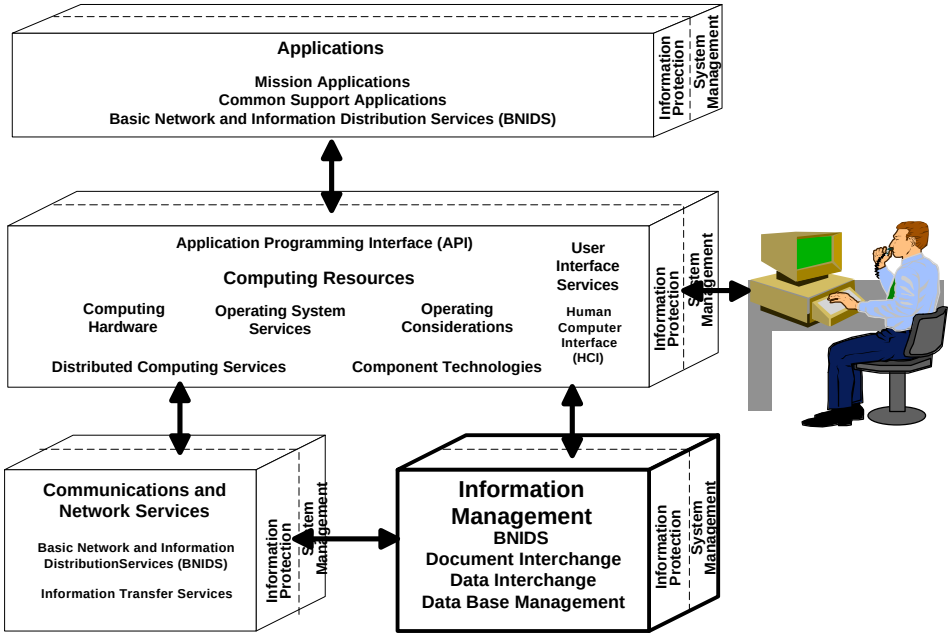


Figure 8-3. Information Management in the Context of the DOD Technical Reference Model

Information management is a process improvement effort that must address information requirements, the aggregation of which become the DON Information Architecture. It also must address information interoperability which is the condition achieved between systems when information or services are exchanged directly between systems and/or their users.

8.1 DOD Policy

8.1.1 Information Interoperability

DOD Directive 4630.5 “Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C^3I) Systems,” requires interoperability between C^3I and interfacing systems. The draft revision to 4630.5, “Information Interoperability,” currently in staffing, expands the scope beyond C^3I, implements the Clinger-Cohen Act, and directs participation in the Defense Information Infrastructure effort. The Joint Chiefs of Staff (JCS) defines interoperabity as the condition achieved between systems when information or services are exchanged directly and satisfactorily between the systems and/or their users.

8.1.2 Information Management

Basic DoD Information Management Program policy is established in DoD Directive 8000.1, “Defense Information Management (IM) Program.” The directive also assigns implementation responsibilities. Among the policies established are (direct quotes):

- Accurate and consistent information shall be made available to decision makers expeditiously to effectively execute the DoD missions
- Data and information shall be corporate assets structured to enable full interoperability and integration across DoD activities

- Identification and validation of process improvements shall be based on DoD-approved activity models that document functional processes and associated data models that document data and information requirements, including integration of information from other functional areas
- Approved DoD-wide methods, approaches, models, tools, data, information technology, and information services shall be used
- Standard DoD data definitions shall be used for all information systems, to include the interfaces between weapon systems and the information systems
- Information systems shall be based upon a model of information needs
- Design by prototyping, in a generally defined strategy, as the preferred course
- Acquire, to the extent practical, information technology components from the centrally-managed DoD-wide information technology repository

8.1.3 Data Administration

DoD Directive 8320.1, "DoD Data Administration", establishes policy that defines requirements for data standardization and data modeling. DoD Directive 8320.1 applies to all information systems of the Navy and Marine Corps, whether or not these systems share data with other systems. DoD data administration is implemented to (direct quotes):

- Support DoD operations and decision making with data that meets the need in terms of availability, accuracy, timeliness and quality
- Structure the information systems in ways that encourage horizontal and vertical sharing of data in the DoD
- Include procedures, guidelines, and methods for effective standards, modeling, and configuration management
- Implement data administration aggressively in ways that provide clear, concise, consistent, unambiguous, and easily accessible data DoD-wide
- Standardize and register data elements to meet the requirements for data sharing and interoperability among information systems throughout the DoD
- Use applicable Federal, national, and international standards before creating DoD standards

DoD Directive 8320.1 seeks to levy the burden and cost of conversion to DoD standard data, regardless of the origin of the requirement for information on the Military Department responsible for the development of the nonstandard data.

DoD Directive 8320.1 identifies the roles and responsibilities of the Component Data Administrator (CDAd). The DON CDAd is responsible for facilitating the implementation of 8320 policy. The DON CDAd represents the DON at DoD-level data administration committees and working groups.

Best Practices

The DON will participate in the DoD data administration process.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DoDD 8320.1 DoDD 8320.1-M DoDD 8320.1-M-1	Implementation Plans			
Activities, Platforms, Operational Environments		Information Producers and Data Base Developers			

Table 8-1. Data Administration Implementation

Note

Implementation Plans – the System Commands (SYSCOMs), Project Engineering Offices (PEOs), System Executive Offices (SEOs) and Program Managers (PMs) should ensure that implementation plan(s) support directives and instructions dealing with data acquisition, information management, data administration, and information interoperability.

8.2 Information Architecture

Information requirements are those necessary to accomplish assigned missions. These requirements are the basis for the DON Information Architecture.

There are three types of architectures – operational, systems and technical – identified in the DoD Joint Technical Architecture (JTA). The DoD C4I Integration Support Activity (CISA) C4ISR Architecture Framework provides the rules, guidance, and product descriptions for developing and presenting these respective architectures. Operational architectures are used to establish the Information Exchange Requirements (IERs) necessary for an organization to perform its assigned missions and objectives. These IERs are consistent with the requirements of JV2010 and the mission-to-information requirements mapping required by the Clinger-Cohen Act. System architectures translate operational needs into specific technologies and systems that are compliant with the requirements of the DII/COE. The Technical Architecture Framework Information Management (TAFIM), the JTA, and this ITSG provide the approved technical components for use in systems development.

The Universal Joint Task List (UJTL), provides a listing of tasks associated with Joint warfare. Additional tasks that are component specific are contained in the Navy Task List and the Marine Corps Task List. Theater and Component Commanders use these lists to select Mission Essential Tasks and associate these tasks with conditions (physical, military and civil) that may affect the performance of them. Information on these conditions provides the basis for conducting military operations. Each task or activity has associated essential elements of information that are maintained in databases and provide a foundation for data exchange. Figure 8-4 shows the relationship between mission, activities, and data. The need is to synchronize the databases and develop common data formats afloat and ashore.

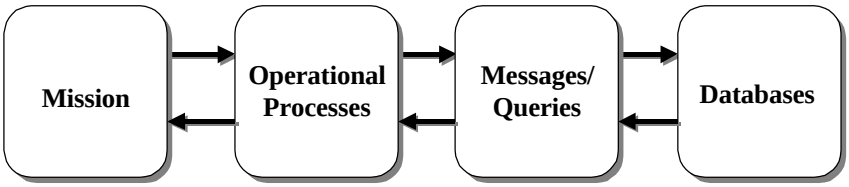


Figure 8-4. Information Requirements Definition

Figure 8-5 depicts an approach for developing a DON Enterprise Information Architecture. Using models to baseline current capabilities provides a practical approach to determine the capabilities of existing system data and databases. Using models to describe the operational data requirements provides an approach to reflect the information requirements of the enterprise.

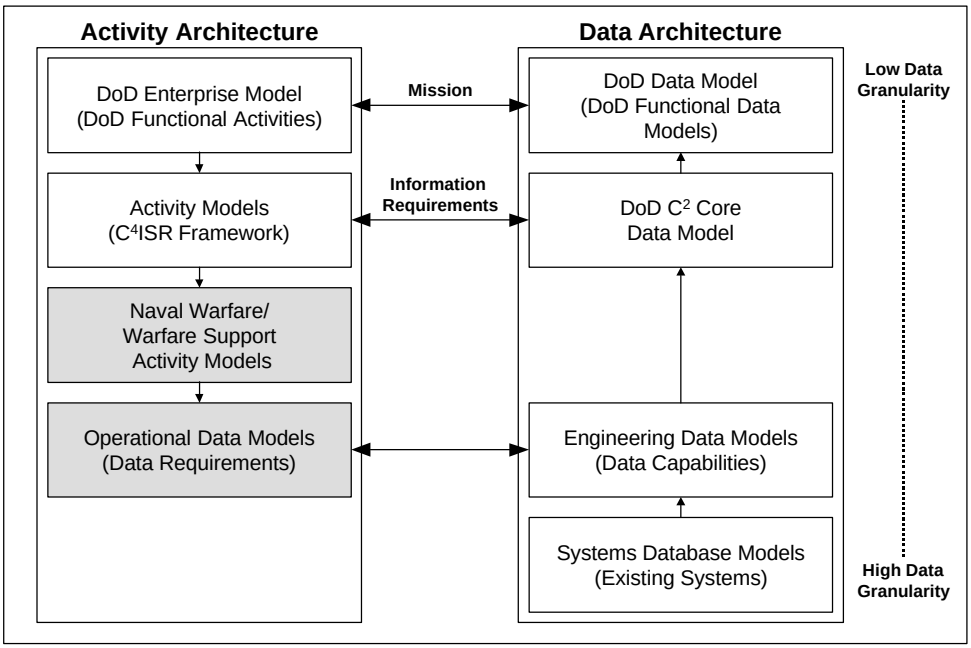


Figure 8-5. Information Architecture

There are two components of the architecture:

- Activity architecture -- decomposes information needs of the enterprise into specific data requirements by using activity models
- Data architecture -- maps existing system database structures and data elements using high level data models

The following describes the two types of modeling which correspond to Activity Architecture and Data Architecture:

Activity Modeling. Enterprise data requirements are developed using Activity Modeling. The activity model is a view of the activities, both automated and manual, that an organization must perform to achieve its mission. Activity models depict the mission area functions of each operational organization. Their primary purposes are to show the information required to support the mission area functions and to identify the functionality required of the mission area applications. They are also used to document and model the activities, processes, and data flows supporting any new system or major update. The

standard format for displaying activities is Integration Definition for Function Modeling (IDEF0) as defined in Federal Information Processing Standard (FIPS) 183.

Activity models have a wide range of uses as shown below:

- Provide a logical representation of related sets of operational activities and their associations
- Provide a means of identifying, capturing, analyzing, decomposing, refining, and documenting operational strategies, rules, and processes
- Act as a set of notations to be defined and manipulated during definition and reengineering of operational functions and processes
- Provide descriptions that enable non-modeling users to understand what functions are involved and assist in their evaluation and improvement
- Provide a basis for defining and justifying data and information requirements
- Provide linkage from organizational missions, strategies, goals, objectives, tactics, and practices to the information systems and data developed to support them

Data Modeling. The data model is for use DON-wide and is developed from the information requirements documented in the activity model. A fully attributed, application-specific data model defines the entities and their data elements, and illustrates the interrelationships among the entities. The data models identify the logical information requirements and metadata that form a basis for physical database schemata and standard data elements. Once implemented, the data is shared using approved information exchange standards. The standard format for displaying a data model is IDEF1X as defined in FIPS 184.

Best Practices

Develop an information architecture responsive to Navy and Marine Corps mission needs that supports the information superiority goals of Joint Vision 2010 and the information initiatives of the Clinger-Cohen Act. Use the C4ISR Architecture Framework guidance and DoD DII/COE principles, guidelines and methodologies in constructing and documenting information architectures.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DII/COE TAFIM/JTA	Implementation Plans			
Activities, Platforms, Operational Environments		Data Base Developers			

Table 8-2. Information Architecture Implementation

Note

Implementation Plans – the SYSCOMs, PEOs, SEOs and PMs should ensure that implementation plan(s) support directives and instructions dealing with data acquisition, information management, data administration, and information interoperability.

8.3 Information Interchange

Information interchange supports the flow of information throughout the network with minimum transformation. These services provide a set of integrated capabilities that the application software entity accesses to obtain standard common operating environment services. The characteristics of the application support services are transparent to the mission and common support applications developer.

8.3.1 Push versus Pull

Basic Network and Information Distribution Services (BNIDS) (Chapter 6) provide the mechanism for information dissemination. The method of dissemination often drives the format and media of the information packages. Four architectural paradigms have been used to model information dissemination and are illustrated in Figure 8-6.

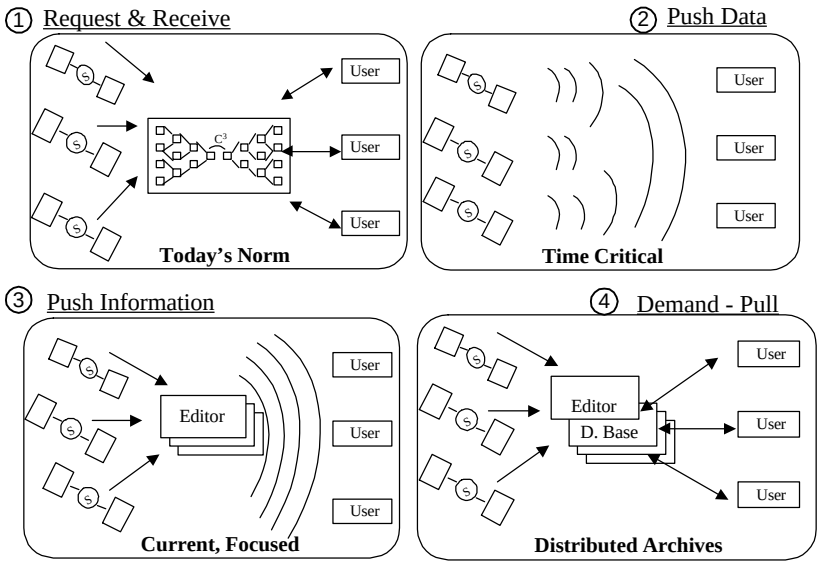


Figure 8-6. Information Dissemination Architectures

1. **Request and Receive.** Each request for data is reviewed and prioritized at the appropriate level in the information support hierarchy as the request travels through the chain of command. Resulting data is delivered back down the chain, often by reversing the steps involved in requesting it. This method is especially appropriate where scarce resources must be rationed, or where special security protection is required for an information collector. Example: sending a Request for Intelligence Information (RII) .

2. **Push Data.** Sensors and data collectors distribute data directly to users, often in a raw or unprocessed condition. The data users must be equipped to receive and process the pushed data. This method is especially appropriate for simple data which is highly time

critical or perishable. Examples: navigation data furnished via global positioning system, direct dissemination of ELINT reports.

3. **Push Information.** Sensor and data collector outputs are fused by an editor into a composite representation; the editor then selects and forwards appropriate information in each of many channels. Each channel is oriented toward a particular group of users and operations. The editor's function is to ensure that the information being forwarded through the channels is correct, complete, germane to the users, and timely. This method is especially appropriate for complex situational data that is time critical or perishable. Example: a televised weather report or news broadcast.

4. **Demand Pull.** This is an on-line reference service. Large archives of information are actively managed by editors; the archives are stored on distributed servers directly accessible by information users. Users directly access the archives when they need archival information. This method is especially appropriate when non-time critical reference data must be made available to a large number of distributed users. Example: a commercial system such as America On Line.

The goal of a Demand Pull information dissemination system is to make a large volume of (archival) data available to a large number of users at user discretion. Certain issues arise which must be addressed by a successful Demand Pull information dissemination system and they are addressed in other chapters of this ITSG.

User Human Computer Interface. The man/machine interface presented to users of the Demand Pull system must be simple, intuitive, predictable, and not require extensive knowledge or training on the part of the user. (Chapter 7)

User Client Terminal. The user terminal equipment must be relatively low cost and multi-functional. (Chapter 7)

Communication Connectivity. Communications connectivity and bandwidth connecting users to the Demand Pull system must be able to support the bursty, high data rate communications required to support user operations. (Chapter 5)

Server Capacity. Server capacity must be sized to handle bursts in level of demand by users, to prevent 'locking out' users from the archived information at critical periods of user operations. (Chapter 7)

Multimedia. Requirements for providing Multimedia archives (text, voice, graphics, sound, images, video, animation) must be defined early because of the impact they have on communications, server capacity, user terminal equipment, user man/machine interface, data modeling, indexing, and search and retrieval. (Chapter 9)

Indexing. Indexing has two distinct parts. First is the location or address of the site (command) where desired information is located, and second is the titling of the information by the site. (Chapter 6)

Search and Retrieval. Browsers must be able to perform effective searches using the search engines and indexes of the archive, and must be able to easily retrieve found information, meeting the user's expectations for quantity, quality, appropriateness, and timeliness of information. (Chapter 6)

Each of the above four described dissemination architectures has wide applicability in both civilian and military situations. Each of the four is appropriate for particular operational and support situations. In the military C^4ISR context, new time critical information has to be pushed. Other push-information situations may include ships in EMCON, or data which is to be distributed to a large number of users, (e.g. ALNAV). Smart push information can be as effective with less communications in certain crisis situations.

8.3.2 Information Discipline

This section discusses information discipline in terms of requirement, scope, technical disciplines, operational disciplines, and the special case of bandwidth management. The objective of information discipline is to assure optimum use of information resources and investments.

8.3.2.1 Requirement

The ability to generate and move information has increased many thousand-fold over the past 20 years. Navy and Marine Corps operations have become more reliant on information technology, the sheer volume of the information threatens to overwhelm our information capability. Unfortunately, the current capability to generate information far exceeds the ability to control and use it effectively. The principal requirement is to manage these volumes of information across the networks to ensure availability during times of crisis. Sets of rules and procedures are required to govern information to prevent gridlocks.

Given this operational significance, information discipline must be standardized and codified with rules of operation and levels of control, similar to other functional disciplines.

8.3.2.2 Scope

The scope of this information discipline effort is extraordinarily wide because virtually all functions rely on the information infrastructure. It includes both the qualitative and quantitative aspects of information operations. It ranges from the standards for information exchange to the operation of the networks for decision support. Both technical and operational disciplines are included.

8.3.2.3 Technical Disciplines

Technical interface standards, which define rules for electronic connectivity and interoperation, represent specialized forms of information discipline. Software standards extend the standards disciplines to the logical levels of signaling, processing, and display. Collectively, these evolving rules and methods represented by technical standards have enabled the information revolution – from international telephone and telegraph networks, ARPANET and the INTERNET to emerging global military networks.

8.3.2.4 Operational Disciplines

With the exception of some physical limitations and the disciplines associated with selected communications and warfare doctrines, the subject of information discipline is undefined. Some communications control measures, such as release authority, precedence and minimize, have been adapted to C4I networks, but they can have only marginal effect unless implemented consistently across the DON enterprise. Where they are implemented, such measures typically produce an abrupt change from saturation to under-utilization. Neither situation represents an optimum use of

resources. In addition, most measures are simply not relevant in a peacetime network where free flowing e-mail messages have become more prevalent than telephone calls. New concepts and methods of information control are required.

8.3.2.5 Methods

While systems were fragmented and used multiple standards, their diversity precluded effective real-time management. However, technologies that enable automated networking of functions can also support selective automation of network management and resultant information discipline. Experience in major exercises and the Gulf War clearly indicate a need for automated, real time monitoring and control of information flows. These methodologies must be built into the support and they must be able to accurately categorize and identify sources of information traffic.

In addition to automating control methods, emphasis must be placed on improving the discipline of originators and users. Experience has proven that once the information is in the networks, controls are of marginal use and can result in serious errors and omissions. The most effective point of information control is at the source.

Most systems and networks already include self-monitoring modules which keep a variety of statistics. These should be modified and expanded to support regional and global analysis and control.

8.3.2.6 Data Rate Management

Data rate refers to the information transfer capacity of a communications medium. It is typically expressed in number of data bits per second. It is often referred to as “bandwidth” even though bandwidth is actually the size of the frequency band given to a communication channel. Typically, the larger the frequency band, the higher the data rate. Hence “data rate’ and “bandwidth” are frequently used interchangeably even though they are not technically the same. Evolving communications and switching technologies have enabled tremendous increases in the effective bandwidth of most media. The degree of increase is shown in Figure 5-3 (Chapter 5), “Evolution of LAN and WAN Data Throughput”, and Table 5-1, “Data Rate Designations”. These figures reflect the technological leaps in data throughput, both in recent implementations and in projections.

On the surface, such increases in capacity would indicate information transfer capabilities that exceed any possible demand and preclude the kind of information gridlocks experienced in previous conflicts. However, that view is superficial in the context of command and control because it disregards factors that collectively increase the need for bandwidth management. These factors include:

- Limitations increase at forward echelons, which need concise, timely information
- Capability disparities exist among interfacing networks and nodes
- Numbers of input and output nodes exponentially increasing
- Information flow controls are often ineffective
- Information generation controls are non-existent
- Excess information extends the decision process
- Excess and conflicting information increases the probability of serious error
- Cost per bit is decreasing, but total information costs are rising

These factors, along with increasing pressures to treat information as a resource, combine to make effective data rate management a higher priority. In the past, communications doctrine and related control mechanisms allocated the limited amount of available bandwidth. However, the effectiveness of those mechanisms deteriorated over time. They were marginally effective in the Gulf War and are irrelevant in many of the network applications today.

New information control and management techniques are required to ensure that the information being generated and transferred is mission relevant, cost efficient and operationally effective. Fortunately, many of the systems being developed have capabilities that can achieve these goals. It is necessary, however, that the management requirements be defined and requisite control measures implemented along with the systems and networks. To this end, future information system development and integration will include the following steps:

- Redefinition of global flow control requirements
- Integration of global control requirements into systems definitions
- Ability of information users to regulate inputs to their systems
- Ability of information producers to meter production and transmission on a precedence basis

8.3.3 Data Interchange Services

Data Interchange Services provide support for the interchange of information between applications, and to and from the external environment. Though areas specific to vertical industry groups are not mentioned in this document, two areas of general applicability are discussed:

- Document Interchange
- File formats

8.3.3.1 Documents

Although the prevailing medium for business documents, paper imposes constraints on document management and control. Document management solutions integrate processes, people, and technology to optimize and automate what were, historically, paper-based business processes. As technology has become more available, the concept or definition of a document has changed. The TOG defines the term document as “a set of information, organized as a unit and intended for human perception.” Ultimately, a document is some amount of structured information that users create, store, retrieve, or manipulate.

Electronic documents often consist of data, text, graphics, images, voice, and video. Consequently, creating, processing, and managing electronic documents encompass many technologies, including imaging, multimedia, databases, text databases, text retrieval, document interchange standards, electronic messaging, and workflow management.

Business documents of an administrative and management nature may be developed and maintained in commercially available word processing, spreadsheet, and presentation software and successfully interchanged and read using format conversion capabilities of these software packages.

Technical documents, such as operations, maintenance, and training publications, are created by various industry and government activities, and delivered and life-cycle maintained with their associated equipment, weapons systems, and platforms. These technical manuals often are version controlled and configuration managed in connection with their associated equipment.

These technical publications should be created, managed, distributed, and used in digital electronic formats suitable for their highly structured technical content and long expected life cycle. The DoD Continuous Acquisition and Lifecycle Support (CALS) initiative has adopted the Standard Generalized Markup Language (SGML) (ISO 8879) as the preferred data standard for technical publications and has defined a military profile for its use within DoD in MIL-PRF-28001.

Best Practices

Commercially available office document software (word processing, spreadsheet, and presentation software), and its embedded translation and conversion functionality, should be used for business, administrative, and management document exchange among disparate environments.

All new technical manuals (TMs), Electronic Technical Manuals (ETMs), and Interactive Electronic Technical Manuals (IETMS) will be acquired in Standard Generalized Markup Language (SGML) format in accordance with MIL-PRF-28001. Proper creation of a document in SGML requires a Document Type Definition (DTD), an SGML data construct defining the structure and content of the type of document to be created as well as the definitions and rules for applying SGML in the authoring process. DTDs are complex and costly to develop but may be created to satisfy a broad range of documents. For this reason, authors and contractors should be encouraged to use existing Document Type Definitions (DTDs) for all TMs/ETMs/IETMs. Navy DTDs are currently stored in the Navy DTD/FOSI Repository (http://navycals.dt.navy.mil/dtdfosi/repository.html).

TM/ETM/IETM delivery to the Government must include the SGML master document, the associated DTD and style sheets, FOSIs (Formatting Output Specification Instance, per MIL-PRF-28001), and filter codes necessary to produce the desired presentation to users. Naval activities are encouraged to also request delivery of a DTD Data Dictionary, defining the meaning of SGML tags used, and a Tagging Conventions document, describing the rules for applying each SGML tag, especially if new or custom DTDs are being used. The information contained within the Dictionary and Conventions documents will be helpful in the maintenance and revision of the TMs and should also be provided to the Navy DTD/FOSI Repository.

Highly dynamic IETMs, i.e., electronic documents whose content is database structured rather than linear or paged and whose presentation is highly dependant on user and data interaction, should also be developed in accordance with MIL-PRF-28001 (SGML). The DTD presented in MIL-PRF-87269 should be used as a guide in the absence of other suitable DTDs. The user interface and presentation format for these IETMs should be developed in accordance with MIL-PRF-87268.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	SGML CALS PostScript SPDL, PDF	SGML XML CALS	SGML XML CALS	SGML XML CALS	
Activities, Platforms, Operational Environments		All			

Table 8-3. Document Exchange Standards

- Standard Generalized Markup Language (SGML) is used for describing both the structure and content of documents. HyperText Markup Language (HTML), an application of SGML, is a current evolving convention for documents on the World Wide Web (WWW).
- Continuous Acquisition and Lifecycle Support (CALS), a Department of Defense initiative, mandates that drawings, technical manuals, and other technical data be created and delivered in standard digital forms. CALS has defined specifications for the exchange of digital data.
- PostScript, Standard Page Description Language (SPDL), and the Portable Document Format (PDF) by Adobe Systems Inc. are acceptable final-form representations for documents. Word processor formats are also acceptable for administrative and management documents.

8.3.3.2 File Formats

File formats are formal structures of file records and layouts that are recognizable and usable by various related products. As a product utility becomes prominent in the industry, other tools and products tend to include the capability to access, use, and create files in the same format as those used by the prominent product.

Note that the use of “file” and “document” in this context is not necessarily text or character-based data. All types of data and media are addressed. Task organization commanders should specify the software file formats to be used during an operation which reflects the common denominator fielded.

The purpose of establishing policy for file formats is not to inhibit product selection but to establish a leverage point for file sharing across the enterprise. Standards are addressed first generally and then by five DON data exchange areas that have specific file formatting standards requirements.

- Geospatial Data Interchange
- Imagery Data Interchange
- Product Data Interchange
- Atmospheric Data Interchange
- Oceanographic Data Interchange

Best Practices

Select products that support the ability to read (import) and create (export) file formats (Table 8-4).

Recommended Implementation

Document Type	Standard/Vendor Format	Recommended File Name Extension	Reference
Plain Text	ASCII Text	.txt	
Compound	Acrobat 2.0	.pdf	Adobe Inc.
Business Document	HTML 2.0	.htm, .html	IETF
	MS Word 6.0	.doc	Microsoft
	MS Word 97		
	Rich Text Format	.rtf	
	WordPerfect 5.2	.wp5	WordPerfect
Briefing	Freelance Graphics 2.1	.pre	IBM
Presentation	MS Powerpoint 4.0	.ppt	Microsoft
	MS Powerpoint 97		
Spreadsheet	Lotus 1-2-3 Release 3.x	.wk3	IBM
	MS Excel 5.0	.xls	Microsoft
	MS Excel 97		
Graphics Imagery	CGM		MIL-PRF-28003, Computer Graphics Metafile (CGM)
	JFIF	.jpeg	Joint Photographic Expert Group (JPEG)
Audio	Wave (WAV)	.wav	
	Audio-Video Interleaved	.avi	
	Audio UNIX (AU)		
Video	MPEG, MPEG2		Motion Picture Experts Group (MPEG)
Internet	HTML 4.0	.htm, .html	IETF
Virtual Reality Model	VRML 2.0	.vmr	Virtual Reality Modeling Language (VRML97, ISO/IEC14772)
Compressed	Zip 2.04	.zip	PKWARE Inc.

Table 8-4. File Formats

Notes

- Compound documents contain embedded graphics, tables, and formatted text. Object Linking and Embedding (OLE) complicates document interchange. Note that not all special fonts, formatting, or features supported in the native file format may convert accurately.

- The current World Wide Web Consortium (W3C) recommendation for HTML is HTML 4.0. HTML 4.0 adds widely deployed features such as tables, applets and text flow around images, superscripts, and subscripts, while providing backwards compatibility with the existing HTML 3.2 standard. (See Section 6.7 for discussion of web standards.)
- VRML 2.0 was improved and adopted as an international specification, VRML97 (ISO/IEC 14722) in December 1997. (See Section 6.7 for discussion of web standards.)
- Technical manuals should be created and delivered to the Navy in MIL-PRF-28001 (SGML). Technical manuals will be stored and managed in SGML in appropriate document management databases and repositories. HTML and XML are limited applications of SGML and are to be used primarily for distribution and presentation of technical manuals to users. Ideally, SGML source data will be converted to HTML for distribution and view.

Desired Form	**Text Standards & Specs**
Electronic Technical Manuals (ETMs)	SGML per MIL-PRF-28001 Use existing DTD or Use new DTD & Request delivery of DTD
Interactive Electronic Technical Manuals (IETMs)	SGML per MIL-PRF-28001 Use MIL-PRF-87269 as guide to DTD User interface per MIL-PRF-87268

Table 8-5. Digital Technical Data Standards for Technical Manual Creation.

Graphics	**Graphics Standards and Specifications**
2-D vector graphics for illustrations & TMs	CGM per MIL-PRF-28003
2-D graphics for hyperlinked illustrations	CGM Level 4 per ATA 2100 V 2.3
Raster (bitmapped) images	MIL-PRF-28002 Type 1 – CCITT.G4

Table 8-6. Graphics Standards for Technical Manual Creation.

Legacy Form	Desired Conversion	Standards & Specs
Technical Manuals	Conversion to SGML	SGML per MIL-PRF-28001 Use existing DTD or Use new DTD & Request delivery of DTD
	Conversion to HTML (Preferred method; supports life cycle management of the converted TM)	Convert first to SGML per MIL-PRF-28001 Use existing DTD or Use new DTD & Request delivery of DTD and Convert SGML to HTML and Deliver SGML, DTD, and HTML
	Conversion to HTML (Alternate method; life cycle management of TM may be difficult due to instability of HTML DTD)	Convert direct to HTML per existing version of HTML DTD and Deliver HTML and the HTML DTD used
	TM Conversion to Raster	PDF per Adobe Systems, Inc or PDL or NIRS/NIFF per Type 3 MIL-PRF-28002 and Indexing per MIL-M-29532
Graphics	Conversion of hardcopy graphics/aperture cards to raster	C4 (JEDMICS) per MIL-PRF-28002 Type 4 or NIFF per MIL-PRF-28002 Type 3
	Conversion of hardcopy or raster graphics to vector	CGM per MIL-PRF-28003
	Conversion of hardcopy or raster graphics to vector with hyperlink capability	CGM, Level 4, per ATA 2100 V2.3

Table 8-7. Digital Technical Data Standards for Legacy Data Conversion

- The following additional standards are recommended for MPEG audio:
  - ISO/IEC 11172-1: 1993 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s—Part 1: Systems
  - ISO/IEC 11172-3: 1993 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s—Part 3: Audio

    - ISO/IEC 11172-3/Cor. 1: 1995 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s—Part 3: Audio Technical Corrigendum.
- The following additional standards are recommended for MPEG2 audio:
    - ISO 13818-1: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems
    - ISO 13818-3: 1995 - Generic Coding of Moving Pictures and Associated Audio Information - Part 3: Audio.
- The following additional standards are recommended for MPEG video:
    - ISO/IEC 11172-1: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s—Part 1: Systems
    - ISO/IEC 11172-1: 1993/Cor. 1:1995 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s—Part 1: Systems Technical Corrigendum 1
    - ISO/IEC 11172-2: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s—Part 2 Video
- The following additional standards are recommended for MPEG2 video:
    - ISO 13818-1: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems
    - ISO 13818-2: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video

8.3.3.2.1 Geospatial Data Interchange

Geospatial services are a collective name for Mapping, Charting, and Geodesy (MC&G) services.

Best Practices

DON navigation and C4I systems, which display cartography, shall be capable of using both National Imagery and Mapping Agency (NIMA) and Electronic Chart Digital Information System (ECDIS) standards.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	MIL-STD-2411 MIL-STD-2407 MIL-STD-2401 DX-90	MIL-STD-2411 MIL-STD-2407 MIL-STD-2401 DX-90	MIL-STD-2411 MIL-STD-2407 MIL-STD-2401 DX-90	MIL-STD-2411 MIL-STD-2407 MIL-STD-2401 DX-90	
Activities, Platforms, Operational Environments		Developers & Engineers			

Table 8-8. Geospatial Service Standards

For mapping, charting, and geodesy (MC&G) services, collectively known as geospatial services, the following standards are recommended:

National Imagery and Mapping Agency (NIMA) Standards

- MIL-STD-2411, Raster Product Format (RPF) - DoD Military Standard used by the National Imagery and Mapping Agency (NIMA) to format raster-based digital products (e.g., Compressed Arc Digitized Raster Graphics (CADRG), Controlled Image Base (CIB), and Digital Point Positioning Data Base (DPPDB)), and is based on National Imagery Transmission Format Standard (NITFS) (MIL-STD-2500A) described below.
- MIL-STD-2407, Interface Standard for Vector Product Format (VPF) - DoD format for NIMA's vector-based products used by geographic information system (GIS) and other DoD systems. VPF standard products include Vector Map (VMap) Levels 0-2, Urban Vector Map (UVMap), Digital Nautical Chart (DNC), VMap Aeronautical Data (VMap AD), Vector Product Interim Terrain Data (VITD), Digital Topographic Data (DTOP), Littoral Warfare Data (LWD), and World Vector Shoreline Plus (WVS+).
- MIL-STD-2401, World Geodetic System 84 (WGS-84) 21 March 1994 - DoD's standard global reference system developed by the DMA. WGS-84 is employed by the NAVSTAR Global Positioning System (GPS) and modern weapons systems. Latitude and longitude data shall use WGS-84 in accordance with CJCSI 3900.01.
- For all other MC&G services (e.g., Digital Terrain Elevation Data (DTED), Digital Bathymetric Database (DBDB)) not captured in the above standards the products in NIMAL 805-1A, NIMA GGI&S List of Products and Services, January 1997 shall be used.

Electronic Chart Digital Information System (ECDIS) Standards – Controlled by International Maritime Organization/International Hydrographers Organization (IMO/IHO)

- DX90 is an interface standard for vector-based cartography subscribed to by all hydrographic agencies worldwide (including National Ocean Survey (NOAA, NOS)), except NIMA. It is functionally equivalent to VPF. The specific database for storage of DX90 data is specified in IHO approved standards (Pubs S-52 and S-57).
- NOAA NOS produces products in BSB (raster specifications) that now include charts of nearly all the coastal areas of the United States.

8.3.3.2.2 Imagery Data Interchange

The NITFS is a DoD and Federal Intelligence Community suite of standards for the exchange, storage, and transmission of digital imagery products. NITFS provides a package containing information about the image, the image itself, and optional overlay graphics. It was developed and mandated by ASD Command, Control, Communications, and Intelligence (C3I) for the dissemination of digital imagery from overhead collection platforms. Guidance on applying the suite of standards can be found in MIL-HDBK-1300A.

Best Practices

Not provided at this time.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	MIL-STD-2500A MIL-STD-188-196 MIL-STD-198-189 MIL-STD 2301 CALS MIL-PRF-28002 MIL-STD-188.198A	MIL-STD-2500A MIL-STD-188-196 MIL-STD-198-189 MIL-STD 2301 CALS MIL-PRF-28002 MIL-STD-188.198A	MIL-STD-2500A MIL-STD-188-196 MIL-STD-198-189 MIL-STD 2301 CALS MIL-PRF-28002 MIL-STD-188.198A	MIL-STD-2500A MIL-STD-188-196 MIL-STD-198-189 MIL-STD 2301 CALS MIL-PRF-28002 MIL-STD-188.198A	
Activities, Platforms, Operational Environments		Developers & Engineers			

Table 8-9. Imagery Service Standards

The following standards are recommended for secondary imagery dissemination:

- MIL-STD-2500A, National Imagery Transmission Format (Version 2.0) for file format
- MIL-STD-188-196, Bi-Level Image Compression
- MIL-STD-188-199, Vector Quantization Decompression
- ISO/IEC 8632: 1992, Computer Graphics Metafile (CGM) as profiled by FIPS 128 and MIL-STD-2301
- CALS MIL-PRF-28002, Raster Graphics Representation in Binary Format
- ISO/IEC 10918-1: 1994, Joint Photographic Experts Group (JPEG) as profiled by MIL-STD-188-198A. Although the NITFS uses the same ISO JPEG algorithm as recommended in Section 2.2.2.1.4.2, the NITFS file format is not interchangeable with the JFIF file format.

8.3.3.2.3 Product Data Interchange

These standards establish data formats for interchanging product description data. These data include not only a graphical depiction, but also manufacturing process information such as materials and surface finishing. Product data also include technical manuals, operating manuals, repair and maintenance guides, training manuals and materials, engineering drawings, parts lists and breakdown structure, and many other data relating to the concept, design, production, delivery, life cycle support and disposal of Navy products.

Best Practices

Not provided at this time.

Recommended Implementation

Standards Table 8-10 presents standards for product data interchange. The DISA Center for Standards uses the following convention to describe the product data interchange specifications:

- National Public Consensus NPC
- International Public Consensus IPC
- Government Public Consensus GPC

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI/US PRO	Digital Representation for Communication of Product Definition Data (revision and redesignation of ANSI/ASME Y14.26M-1989) (Formerly IGES)	ANSI/US PRO/ IPO 100-1996	Adopted (Approved)
GPC	NIST	Initial Graphics Exchange Specification (IGES) (adopts ASME/ANSI Y14.26M-1989) (IGES ver. 4)	FIPS PUB 177:1992	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 1: Overview and Fundamental Principles (formerly Product Data Exchange Specification (PDES))	10303-1:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 11: The EXPRESS Language Reference Manual (formerly PDES)	10303-11:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 21: Implementation Methods: Clear Text Encoding of the Exchange Structure	10303-21:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 31: Conformance Testing Methodology/Framework: General Concepts	10303-31:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 41: Integrated Generic Resources: Fundamentals of Product Description and Support	10303-41:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 42: Integrated Generic Resources: Geometric and Topological Representation	10303-42:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 43: Integrated Generic Resources: Representation Structures	10303-43:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 44: Integrated Generic Resources: Product Structure Configuration	10303-44:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 101: Integrated Application Resources: Draughting	10303-101:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 201: Application Protocol: Explicit Draughting	10303-201:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 203: Application Protocol: Configuration Controlled Design	10303-203:1994	Adopted (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Adopted (Approved)
GPC	DOD	Automated Interchange of Technical Information (Life cycle logistic support of weapon systems)	MIL-STD-1840B of 11/3/1992	Adopted (Approved)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text	MIL-PRF-28001C May,1997	Adopted (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
NPC	ANSI/US PRO	IGES 5.2, Initial Graphics Exchange Specification (Replaces ANSI/ASME Y14.26M-1989)	US PRO/IPO-100 (Nov 1993)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Part Libraries, About 10 Parts in Progress	13584-XX work in TC184/SC04	Informational (Draft)
GPC	NIST	Initial Graphics Exchange Specification (IGES): v. 5.2 OR 6.0	FIPS PUB 177-1 (future)	Informational (Formative)
GPC	DOD			
GPC	DOD			
NPC	ANSI/ASME			

Table 8-10. Product data interchange standards

Notes

- The DoD/CALS Initial Graphics Exchange Specification (IGES) standard, MIL-PRF-28000, is preferred for CAD illustrations, engineering drawings, geometry for numerical control manufacturing, and 3-D Piping information in IGES. The standard is optional for technical manual illustrations. The CALS standard for Computer Graphics Metafile (CGM), MIL-PRF-28003 is preferred for technical manual illustrations. Table 8-11 provides guidance.

Application	Standards & Specs
2-D graphics for use in CAD	IGES V5.3 per MIL-PRF-28000 Class II or STEP per ISO 10303 AP201 or AP 202
Product data CAD/CAM/CAE 3-D vector Product Model	Native CAD format and Neutral format per, MIL-PRF-28000, or IGES per ASME Y14.26 IGES Version 5.3 or STEP per ISO 10303
Ship Design	STEP per following: NSRP Doc 0424 Piping AP NSRP Doc 0425 Electrical/Cableway AP NSRP Doc 0426 HVAC AP NSRP Doc 0428 Outfit and Furnishings AP NSRP Doc 0429 Ship Structure AP

Table 8-11. Product Data Creation

- The IPO Electrical Applications Committee (AEC) Layered Electrical Products Application Protocol (LEP AP) is the CALS preferred IGES specification for representation of electrical products.
- The ISO 10303 Standard for the Exchange of Product Model Data (STEP) standard is a set of interrelated application profiles that define a vocabulary and syntax for the exchange of product data. The scope of ISO 10303 encompasses all aspects of product data that may be collected and exchanged for any product throughout the life cycle. In its current state, ISO 10303 primarily addresses the exchange of material and shape data. ISO 10303 is a standard designed for expansion. As such, a large part of its initial content lays in the conceptual framework from which any topic area or product data may be standardized to exchange data.
- Specific applications included in the current version of STEP concern the exchange of 2-D drafting data (AP 201 Explicit Draughting, AP 202 Associative Draughting) and the exchange of configuration controlled 3-D design data (AP 203 Configuration Controlled Design). Interoperability of data among these application protocols cannot be assured as this has not yet been a design criterion of the STEP standards community. Much of the applications for STEP are still being defined in the form of a number of Application Protocols (APs) still under development.

Related standards. The following standards are related to product data interchange or product data interchange standards:

- MIL-HDBK-1300A, NITFS.
- MIL-STD-2500A, NITF, Version 2.0 for the NITFS.

Recommendations: ANSI/US PRO/IPO 100-1996 (Formerly IGES) is Year 2000 compliant and is recommended except for cases where STEP provides additional capabilities that are lacking in IGES and are critical to the accomplishment of the system. STEP includes IGES's functionality, but is more comprehensive. The CALS IGES specification, MIL-PRF-28000, specifies 4 classes of IGES files: Technical Illustration (I), Engineering (II), Numerical Control Manufacturing (IV), and 3D Piping (V). The CALS specification Class III, Electrical/Electronic, should not be used. For Electrical/Electronics IGES data, ANSI US PRO/IPO 100 Layered Electrical Product Application Protocol should be cited.

IGES products are implemented widely and are likely to be proposed by vendors whether or not a procurement specifies it. In contrast, STEP products must be specified explicitly. If STEP is specified in a procurement, then it should conform to the requirements in the ISO 10303 STEP.

8.3.3.2.4 Atmospheric Data Interchange

The following formats established by the World Meteorological Organization (WMO) Commission for Basic Systems (CBS) for meteorological data and published under the Manual for Codes, Volume 1, Part B, Binary Codes, WMO No. 306.

Best Practices

Not provided at this time.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	FM 92-X-GRIB FM 94-X-BUFR DEF	FM 92-X-GRIB FM 94-X-BUFR DEF	FM 92-X-GRIB FM 94-X-BUFR DEF	FM 92-X-GRIB FM 94-X-BUFR DEF	
Activities, Platforms, Operational Environments		Developers & Engineers			

Table 8-12. Atmospheric Data Interchange Standards

- FM 92-X-GRIB - The WMO Format for the Storage of Weather Product Information and the Exchange of Weather Product Messages in Gridded Binary (GRIB) Form. GRIB was developed for the transfer of gridded data fields (including spectral model coefficients) and of satellite images. A GRIB record (message) contains values at grid points of an array, or a set of spectral coefficients, for a parameter at a single level or layer as a continuous bit stream. It is an efficient vehicle for transmitting large volumes of gridded data to automated centers over high speed telecommunication lines using modern protocols. It can equally well serve as a data storage format. While GRIB can use predefined grids, provisions have been made for a grid to be defined within the message.
- FM 94-X-BUFR - The WMO Binary Universal Format for Representation (BUFR) of meteorological data. Besides being used for the transfer of data, BUFR is used as an on-line storage format and as a data archiving format. A BUFR record (message) containing observational data of any sort also contains a complete description of what those data are: the description includes identifying the parameter in question, (height, temperature, pressure, latitude, date, and time), the units, any decimal scaling that may have been employed to change the precision from that of the original units, data compression that may have been applied for efficiency, and the number of binary bits used to contain the numeric value of the observation. BUFR is a purely binary or bit oriented form.
- Data Exchange Format (DEF) - Appendix 30 to the Tactical Automated Weather Distribution System (TAWDS)/Integrated Meteorological System (IMETS) Implementation Document for Communication Information Data Exchange (CIDE).

8.3.3.2.5 Oceanographic Data Interchange

Standard transfer formats are required for the pre-distribution of oceanographic information. WMO GRIB and the BUFR file transfer formats are used for this purpose. The GRIB and BUFR extensions include several extensions, including provisions for additional variables, additional originating models, a standard method to encode tables and line data; a method to encode grids (tables) with an array of data at each grid point (table entry); and a method to encode multiple levels in one GRIB message. There is also a possible need to incorporate a method for vector product data.

Best Practices

None provided at this time.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	FM 94-X-BUFR	FM 94-X-BUFR	FM 94-X-BUFR	FM 94-X-BUFR	
Activities, Platforms, Operational Environments		Developers & Engineers			

Table 8-13. Oceanographic Data Interchange Standards

- FM 94-X-BUFR - The WMO Binary Universal Format for Representation (BUFR) of oceanographic data is appropriate for discrete oceanographic observations at a location, but it is inappropriate for gridded fields produced as a result of a model run, such as wave heights, sea surface, temperature, etc., In those cases the same formats used for Atmospheric Data Interchange FM 92-X-GRIB should be used.

8.3.4 Messages

8.3.4.1 Bit-Oriented Message Standards

The J-series family of Tactical Data Link (TDL) allows information exchange using common data element structures and message formats to support time critical information. Users include Air Operations/Defense, Maritime, Fire Support, and Maneuver Operations. The J-series family consists of Link 16, Link 22, and the Variable Message Format. Interoperability is achieved through the common use of the J-series family of messages and data elements. The policy and management of this family is described in the Joint Tactical Data Link Management Plan (JTDLMP), dated April 1996.

Best Practices

DON users shall address new message requirements using these messages and data elements or use the message construction hierarchy described in the JTDLMP.

Recommended Implementation

The JTIDS/TADIL J/Link 16 standards listed below are hierarchical in nature, and the relationships of these separate standards are explained in Operational Specification (OS) 516.2. The governing document for DON implementation of TADIL J message formats is OPSPEC 516.2. OPSPEC 516.2 references sections of MIL-STD-6016 for system implementations but adds more stringent requirements and formats. OS-516.2 references sections of MIL-STD-6016 for system implementations. Link 11/TADIL A will be subsumed into Link 16 and implementations of Link 16 are required to be interoperable with Link 11/TADIL A message standards.

Baseline	MIL-STD-6011A DoD Interface Standard Tactical Digital Interface Link (TADIL) A Message Standard, 24 January 1997 Navy Tactical Data Systems Model 4, Link 11 Operational Specification OS-411.3, Revision 3, 20 February 1997 MIL-STD-6004 DoD Interface Standard Tactical Digital Interface Link (TADIL) C Operational Interface Standard Navy Tactical Data Systems Link 4 Operational Specification OS-404.1 with Change 5, 20 December 1988 Includes JTIDS/TADIL J/Link 16 target standards
Target	JTIDS Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 3 August 1994 MIL-STD-6016 DoD Interface Standard Tactical Digital Interface Link (TADIL) J Message Standard, 7 February 1997 LINK 16 Operational Specification OS-516.2 Revision 2, 20 February 1997 STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 2 March 1990 VMF Technical Interface Design Plan, - Test Edition (TIDP-TE), Reissue 1 February 1995
Emerging	STANAG 5516, Edition 2, is currently under development at JIEO for delivery to the NATO Data Link Working Group (DLWG). STANAG 5552, Edition 1, Tactical Data Exchange - LINK 22 (Undated) is the Configuration Management baseline document. VMF Technical Interface Design Plan - Reissue 2, is currently undergoing development at JIEO.

Table 8-14. Bit-Oriented Message Standards

JTIDS will soon be supplemented by the Multi-functional Information Distribution System (MIDS). Message format standards for MIDS will not change from those of the JTIDS. Message and data element standards must be independent of the information transfer standards, protocols, and profiles. Refer to Chapter 5 of this document for information transfer standards.

STANAG 5516, Edition 2, is currently under development at the DISA Joint Integration and Engineering Office (JIEO) for delivery to the NATO Data Link Working Group (DLWG).

STANAG 5552, Edition 1, Tactical Data Exchange - LINK 22 (Undated) is the Configuration Management baseline document.

8.3.4.2 Character-Oriented Message Standards

United States Message Text Format (USMTF) messages are jointly agreed, fixed-format, character-oriented messages that are man-readable and machine-processable. USMTF is the mandatory standard for record messages when communicating with the Joint Staff, combatant commands, and service components. The OS-OTG is in the process of being subsumed within the Variable Message Format (VMF) standard.

Baseline	Includes target Standard Operational Specification For Over-the-Horizon Targeting Gold (OS-OTG), Revision C - 1 August 1997 (Change 1 Scheduled Oct 98)
Target	MIL-STD-6040, United States Message Text Format (USMTF)

Table 8-15. Character-Oriented Message Standards

8.4 Database Management

This section provides the DON information management approach for life-cycle data management. Topics discussed include the following:

- Database Management Process
- Database Interoperability
- Database Documentation
- Database Management Systems

8.4.1 Database Management Process

The DON approach for achieving and maintaining database interoperability is to focus existing resources to:

- Identify and integrate user and system data requirements
- Register existing system data elements to use applicable standards
- Institute and manage DON approved data standards; recommend to DoD for approval as DoD data standards
- Implement approved standards in all systems
- Provide consistent, authoritative reference data
- Document and report information problems and solutions

The five interrelated sub-processes shown in Figure 8-7 provide a life cycle approach for database management across the DON enterprise.

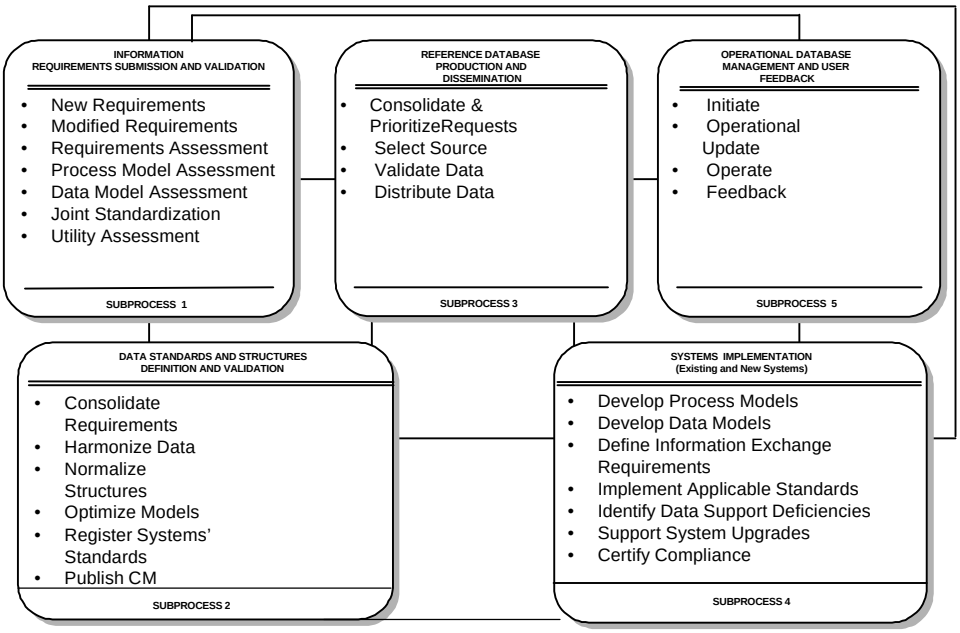


Figure 8-7. Development Approach

Coordinated implementation of these sub-processes provides effective and efficient life-cycle data management. It also enables the DON enterprise to gain better utility of existing resources and an increased return on IT investment. Each of the sub-processes is explained in the following paragraphs.

8.4.1.1 Information Requirements Submission and Validation

Provides the method by which validated operational requirements for information (both for new and existing systems) are established.

Fleet inputs are consolidated by the Fleet CINCs reflecting mission requirements that must be supported by new, emerging, and migration systems. These are brought together and validated by the resource sponsors. This subprocess establishes information collection priorities, identifies potential authoritative sources, optimizes resources, and obtains commitment to development and maintenance of new information standards.

8.4.1.2 Data Standards and Structures Definition and Validation

Provides the method to consolidate system information requirements into "essential elements of information" optimized for tactical Naval warfare and support infrastructure.

The data standards determine how data elements are named, defined, and managed. Registration of system data elements is a foundation for data standardization, database integration, and database synchronization.

8.4.1.3 Reference Database Production and Dissemination

Provides the method by which functional information managers produce and disseminate reference data.

This addresses what source is authoritative, who should produce the data, how data structures are defined, and how data is distributed. The data element fill or content varies according to the dataset to which the elements are assigned and the area of operations. Using validated data from authoritative national, service or theater producers will fill data elements for datasets that are common to all users. The data elements that define dynamic situations, such as target tracking, will be filled at the appropriate operating level.

Since several levels and categories of classified data are available, data security is vital. Access control policies and accountability requirements for the data are the responsibility of the respective producers.

8.4.1.4 Systems Implementation

Provides the method to implement approved information standards in legacy and migration systems.

To ensure intersystem information interoperability, system developers will comply with data and interface standards. Management of existing systems that are undergoing modernization should include a transition plan to DoD and DON data standards.

Program Managers will direct their Component Software Support Centers and Software Support Activities (SSC/SSAs) to work with the DON Data Administrator in registering their data element formats in the Defense Data Dictionary System (DDDS). Baseline DON and DoD standards will be derived from those elements that are registered. This will simultaneously provide unambiguous interface definitions for other systems (i.e., those systems that need to exchange data) to ensure optimal data flow. A Functional Information Manager (FIM) will be assigned to oversee the establishment and maintenance of a quality data base.

8.4.1.5 Operational Database Management and User Feedback

Provides the method by which operational users manage changes to reference data, how they supplement with specific or local data, and how they provide feedback on the validity and utility of data.

Data fill will not be completed for all data elements that are provided by the operational commanders. The DON process will be to register requests for data fill requirements and provide feedback on those requests. The goal is to complete those data fill requests that reflect optimal use of production assets in support of operational needs.

Once the common reference database is distributed by the FIM, battle group and local data is added to optimize operational databases. The operational databases are a combination of the basic loads tailored with regional and local fill. Figure 8-8 provides a methodology for documenting and reporting information management problems and solutions.

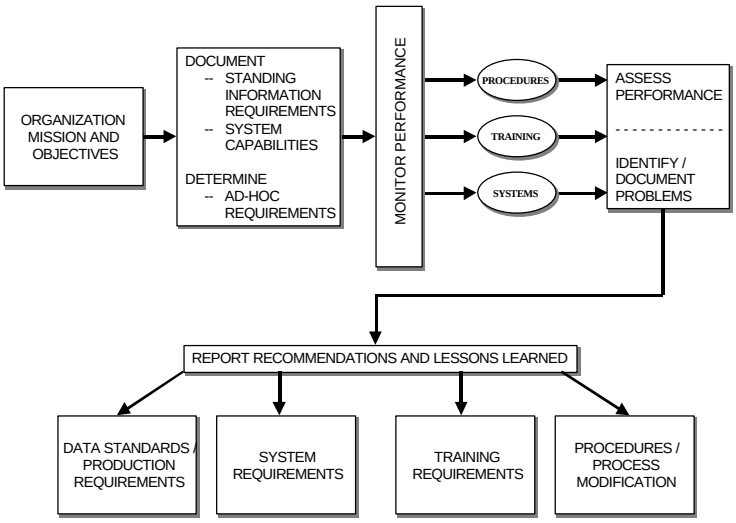


Figure 8-8. Information Improvement Process

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DoDD 8000.1 DoDD 8120.1 DoDD 8320.1 DoDD 4630.5 Review OPNAVINST 9410.5 Review OPNAVINST 9410.6 Review MCO 3093.1 Review NAVINTCOMINST 3890.1 Review OPNAVINST 3430.23 Review OPNAVINST 3140.54 Review OPNAVINST 3140.55	Implementation Plans*			
Activities, Platforms, Operational Environments		Information Producers and Data Base Developers			

Table 8-16. DON Information Management Implementation

* Implementation Plans – the SYSCOMs, PEOs, SEOs and PMs should ensure that implementation plan(s) support directives and instructions dealing with data acquisition, information management, data administration, and information interoperability.

8.4.2 Database Interoperability

Understandable descriptions of the database are key to data interoperability. Figure 8-9 provides an overview for defining and harmonizing the DON data environment. These products provide the enterprise baseline for registration in the DDDS.

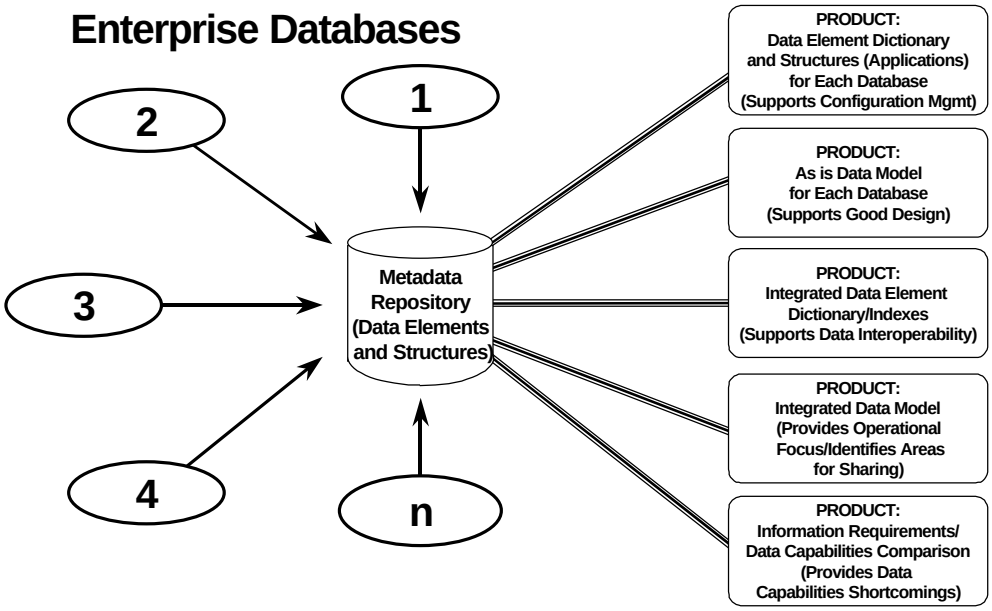


Figure 8-9. Methodology for Achieving and Maintaining DON Information Interoperability

8.4.2.1 Establishing and Maintaining a Baseline (Registration)

Figure 8-10 provides a methodology for capturing knowledge in order to assess the impact or goodness of proposed DoD data standards. Establishing a baseline requires a consistent process by which to organize data elements, define attributes, and select data sources.

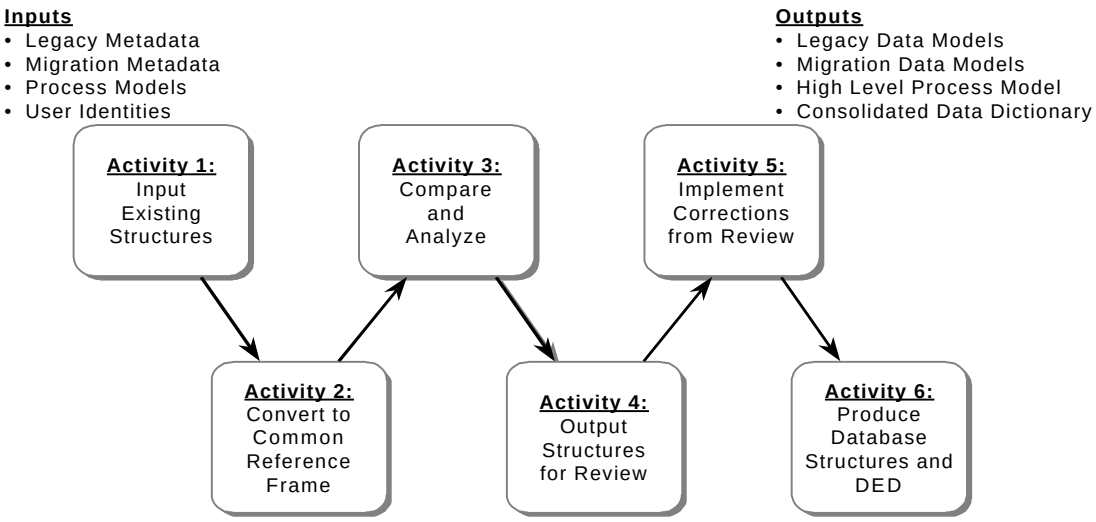


Figure 8-10. Capturing Metadata in a Common Format

8.4.2.1.1 Organizing Data Elements

Database structures are used to organize data elements to support applications. Figure 8-11 illustrates how data elements are grouped to define an area of interest. The example shows a grouping that defines the cargo of a merchant ship.

Table Name: MER_SHIP_CARGO

	SCONUM [pf]	CHAR	6
	CAPBLTY_SELF_SUS	CHAR	1
	LENGTH_RORO_M	99999	
	LENGTH_RORO_FT	99999	
	NBR_RAMPS	99	
	CAPCTY_DWT_CARGO_MTON	99999999.9	
	CAPCTY_DECK_SPACE_SQM	999999	
	CAPCTY_DECK_SPACE_SQFT	99999999	
	NBR_CARGO_HOLDS	99	
	CAPCTY_CARGO_HOLDS_CUM	999999	
	CAPCTY_CARGO_HOLDS_CUFT	99999999	
	CAPCTY_GRAIN_CUM	999999	
	CAPCTY_GRAIN_CUFT	99999999	
	NBR_CARGO_TANKS	99	
	CAPCTY_GAS_CUM	999999	
	CAPCTY_GAS_CUFT	99999999	
	CAPCTY_LIQUID_CUM	999999	
	CAPCTY_LIQUID_CUFT	99999999	
	CAPCTY_REFRG_CUM	999999	
	CAPCTY_REFRG_CUFT	99999999	
	CAPCTY_CONTAINER_TEU	999999	
	CONTAINER_RMKS	CHAR	25
	NBR_CONTAINERS	9999	
	NBR_AUTOS	9999	
	NBR_BERTH_PASS	9999	
	NBR_PASS_TOT	99999	
	CAPCTY_LIFT_COMB_MTON	99999999.9	
	CAPCTY_LIFT_DEV_MAX_MTON	99999999.9	
	NBR_LIFT_DEV	99	
	NBR_PUMPS	99	
	RATE_PUMP_MTPH	99999	
[n]	MER_SHIP_CARGO_SK [a]	NUMB	14
[n]	MERCHANT_SHIPS_SK [a]	NUMB	14

Figure 8-11. Data Element Table

8.4.2.1.2 Defining Data Attributes

Data elements must be defined to reflect functional context. Figure 8-12 provides an example of some of the attributes used to define a data element.

Access Name: SCONUM
Long Name: SHIP CONTROL NUMBER
Definition: The ship control number assigned to a ship by the Navy Operational Intelligence Center (NAVOPINTCEN) for record identification purposes.
Type: VARCHAR2 **Length :** 6
Unit of Measure:
Domain Low :
Domain Value Identifier(s) and Definition(s):
Database: NID V3
Table Usage : MERCHANT_SHIPS,
MER_SHIP_ALT_NAMES,
MER_SHIP_ANTENNA,
MER_SHIP_CARGO,

Figure 8-12. Data Element Description

8.4.2.1.3 Functional Information Managers

To implement data administration it is necessary to identify DON Functional Information Managers (FIM) to assist in developing procedures for both inter-and intra-functional data standardization and the broader goal of information interoperability.

8.4.2.1.4 Authoritative Data Sources

Functional Information Managers should establish close working relationships with authoritative data sources for their respective reference data, e.g. C3, intelligence, logistics, personnel, medical, and acquisition.

8.4.2.1.5 Data Repositories

A data repository contains the metadata (data about data) associated with an enterprise or functional area. The Defense Data Dictionary System (DDDS), operated and maintained by DISA, contains the DoD archived, developmental, candidate disapproved and approved DoD data standards. The Secure Intelligence Data Repository (SIDR), sponsored by the Defense Intelligence Agency and the National Security Agency (NSA), is under development to maintain classified standard and candidate standard DoD data elements.

8.4.2.2 Achieving Information Interoperability

Four important efforts that will lead to information interoperability are the following:

- Definition and implementation of database segments
- Data element standardization as part of migration database integration
- Database synchronization
- Data warehousing and mining

8.4.2.2.1 Definition and Implementation of DII COE Database Segments

DON is supporting the development of DII COE database segments. One such effort is JMCIS. Software modules are being submitted to the DISA Shared Data Environment (SHADE) for run time compliance testing. As segments are produced, their associated data will have to be normalized and synchronized.

8.4.2.2.2 Data Element Standardization as part of Migration Database Engineering

Individual system databases should be normalized to reach the state of one fact, one place. Databases within a functional area should be harmonized to provide data quality and efficiency of life cycle data maintenance. Figure 8-13 illustrates how legacy databases can be mapped to migration databases to ensure information requirements continue to be satisfied by new systems. Mapping and matching of non-standard data to DoD standards will be done per DoD 8320.1-M-1.

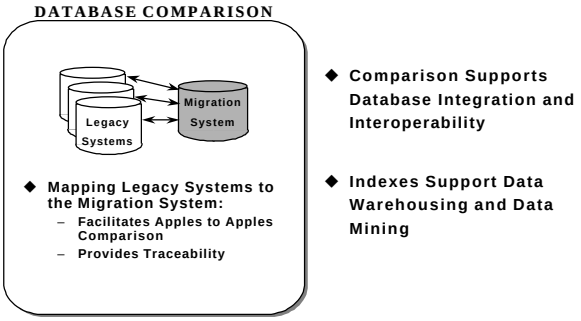


Figure 8-13. Data Element Comparison and Linking

8.4.2.2.3 Database Synchronization

Database synchronization can be achieved by mapping the data elements and aggregating the databases into a single model. Figure 8-14 shows a telecommunications links and nodes model that was developed as part of an information warfare data standardization study involving multiple databases. Each of the different databases reflects their command's view of their mission and organization. Aggregation of the separate views into an integrated view provides a framework for sharing and interoperability.

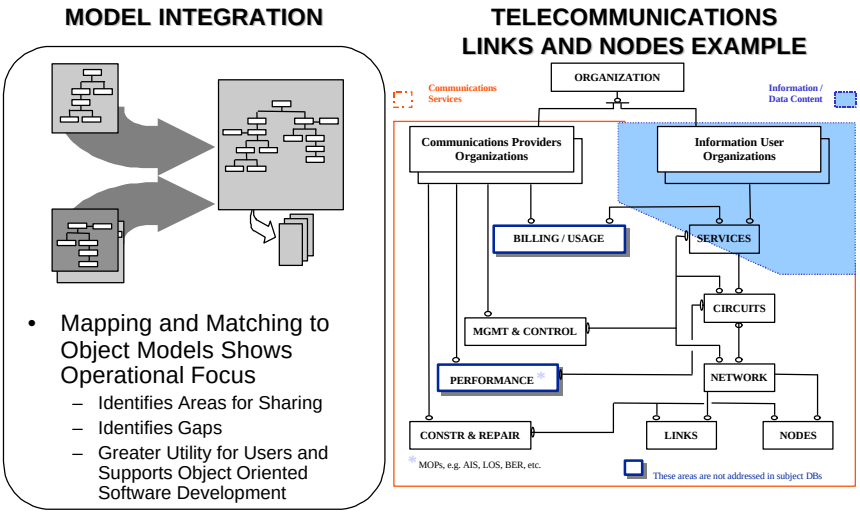


Figure 8-14. Database Synchronization

8.4.2.2.4 Data Warehousing and Mining

Data warehousing and mining strategies will be facilitated by database normalization, functional harmonization, and cross-functional synchronization. A data warehouse is an informational database implementation used to store sharable data sourced from operational databases-of-record. It is typically a subject database that allows users to tap into an operational or functional command's vast store of operational data to gain access to data/information.

Data mining is a technique using software tools geared to the user who typically does not know the specific data they are searching for, but are looking for particular data patterns or trends. Data mining is the process of sifting through large amounts of data to produce data content relationships.

8.4.3 Database Documentation

Documentation of systems databases in a common format provides a basis for functional process improvement and cross-functional sharing. Documentation provides a context for developing data metrics. There are commercial and government off-the-shelf tools to provide a means to capture the data to support information management and information engineering.

Best Practices

DON information management policy will be implemented through the DON CIO for all warfare and warfare support communities. DON systems managers will produce and maintain data

element dictionaries and data structures in approved DoD format. Copies will be provided to the DON Component Data Administrator for coordination with DoD components.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DII/COE TAFIM/JTA DoDD 4630.5 DOSI 4630.8 DoDD 8120.1 DoDD 8320.1 FIPS 183 FIPS 184	Implementation Plans			
Activities, Platforms, Operational Environments		Data Base Developers			

Table 8-17. DON Data Base Documentation Guidance

Note

Implementation Plans – the SYSCOMs, PEOs, SEO's and PMs should ensure that implementation plan(s) support directives and instructions dealing with data acquisition, information management, data administration, and information interoperability.

8.4.4 Database Management Systems

Data management services give applications access to structured data in a distributed environment. The ISO Structured Query Language (SQL) standard is the primary interface to relational databases, but the SQL Access standard extends this interface to access databases over a network.

Database technology is evolving rapidly. Data storage and access have matured from simple flat files into sophisticated database management systems (DBMS) based on hierarchical, networking, relational, and multidimensional data models. Object-oriented technology bases the object management system on the object model. Databases continue to grow exponentially in size, from hundreds of gigabits to multi-terabyte.

Current and future trends for databases focus on DBMSs based on the relational model and the object model or a hybrid of the two. The hybrid DBMS may extend the relational model to support aspects of the object model, such as complex data types (voice and image) or encapsulation (the packaging of an object's data and processes). Conversely, the hybrid DBMS may extend the object model to support aspects of the relational model, such as SQL.

The various Relational Database Management Systems (RDBMS) vendors are currently examining the capability to construct multidimensional “cubes” as a strategic base function to add to RDBMS database engines. Increased market demand for decision support systems (DSSs) and the complex data analysis inherent in DSS has provided the momentum for adding this capability.

The Internet/intranet has increased the need for DBMSs to support more complex data types, such as audio and video. In fact, DBMS vendors are interested in providing Web server capabilities within their databases, relieving the need to have both a web server and a database server.

Each data model provides benefits that are specific to business needs. For example, DSSs may be best served by DBMSs based on the relational or multi-dimensional models. Support for complex data types, such as full motion video, may be better suited for DBMSs based on the object model. Guidelines for selecting a DBMS model are based on the type of data and its relationships (Figure 8-15).

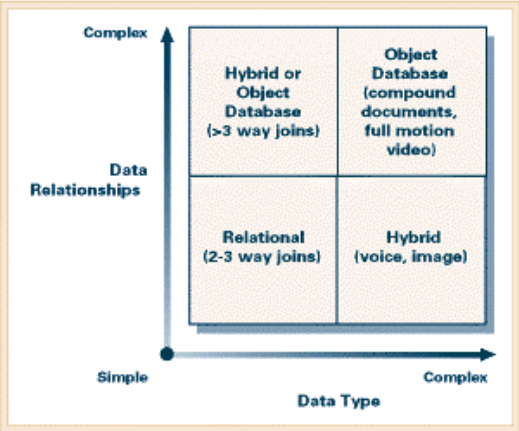


Figure 8-15. Guidelines for Selecting a DBMS Model

In today’s business environment, data is typically spread across multiple DBMSs, hardware, and operating system platforms. Access to an enterprise’s data can be complex. Two areas that have addressed this complexity are standards and middleware.

8.4.4.1 Relational Database Management Systems (RDBMSs)

Several RDBMSs provide Client /Server products and support for some aspects of the object model. The Open Group (TOG), through its XA specification, defines a standard interface between RDBMSs and transaction processing systems. TOG’s specification, based closely on the ISO standard for SQL, provides a common SQL for data access and manipulation. The Remote Data Access (RDA) specification defines the formats and protocols required for an SQL application to communicate with a remote database (Figure 8-16).

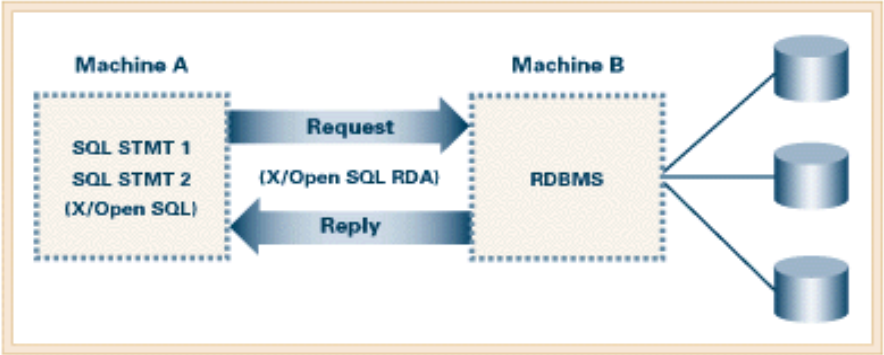


Figure 8-16. The Open Group SQL and RDA

Interoperability between relational databases became a problem when multiple RDBMSs were introduced in the market. The Open Group and the SQL Access Group (SAG) made progress toward RDBMS interoperability when they jointly published two key specifications: the SQL RDA specification and an updated version of SQL. This update combined the efforts of SAG and TOG to provide a unified standard.

Best Practices

In accordance with FIPS Pub 127-2:1993, Database Language for relational DBMSs, select a RDBMS that supports both the entry level SQL standards and The Open Group's XA standards. The API recommended for both database application clients and database servers is the Open Data Base Connectivity, ODBC 2.0.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	ISO SQL ISO RDA TOG SQL TOG RDA TOG XA TOG SQL CLI DB2 ODBC 2.0	ISO SQL ISO RDA TOG SQL TOG RDA TOG XA TOG SQL CLI DB2 ODBC 2.0	ISO SQL ISO RDA TOG SQL TOG RDA TOG XA TOG SQL CLI DB2 ODBC 2.0	ISO SQL ISO RDA TOG SQL TOG RDA TOG XA TOG SQL CLI ODBC 2.0	
Activities, Platforms, Operational Environments		Data Base Developers			

Table 8-18. Relational Database Management Systems

TOG's RDA and IBM's Distributed Relational Database Architecture (DRDA) offer a different approach to Client /Server database interoperability. Through DRDA, IBM provides interoperability among its relational database managers found on its different hardware and operating system platforms. DRDA does not focus on general industry-wide interoperability and, therefore, is not recommended.

8.4.4.2 Object-Oriented Database Management Systems

Object-oriented database management systems (OODBMSs) are used primarily for small to medium systems that require extensive use of nontraditional data types used in engineering (computer-aided design/computer-aided manufacturing [CAD/CAM]), manufacturing (CIM), geographic information systems, and, more recently, Internet/intranet multimedia applications. Although several standards organizations are working on standards for object management for databases, these standards lag behind RDBMS standards.

The Object Data Management Group (ODMG) is a consortium of vendors and interested parties who collaborate to develop and promote standards for object storage. The current standard published by the consortium is ODMG Release 2.0. Its purpose is to ensure the portability of applications across different DBMSs. ODMG is built upon existing standards wherever possible. The ODMG specification is a set of components that include an Object Model, an Object Definition Language, an Object Query Language, and Language Bindings to Java, C++, Smalltalk.

Best Practices

Select products that comply with ODMG 2.0. Alternatively, minimize risk by selecting an OODBMS supplier that participates in, or supports, the following standards organizations: ODMG, Object Management Group (OMG), and the ANSI X3 subgroup, Object-Oriented Database Task Group.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	ODMG 2.0	ODMG 2.0	ODMG 2.0	ODMG 2.0	SQL3
Activities, Platforms, Operational Environments		Data Base Developers			

Table 8-19. Object-oriented database management systems

8.4.4.3 Database Access

Database access middleware, also referred to as database gateway middleware, resides between the client application and the supplier DBMS or file system. Database access middleware provides the client application and end user with a single method and view of accessing data in a heterogeneous database environment. The method can vary from APIs to fourth-generation languages (4GLs) or to gateways (point-to-point, SQL, or universal).

Standard APIs are preferred for applications because APIs are more portable and interoperable. 4GLs and gateways are well suited for end-user access to heterogeneous databases. Point-to-point and SQL gateways tend to support limited databases, but universal gateways support various DBMSs and file systems.

Sun Microsystems' Java language specification for developing Internet/intranet applications has provided impetus for the development of the Java Database Connectivity (JDBC) API. This API provides a standard SQL database access interface from a Java application. These JDBC drivers can be categorized as:

- JDBC- open database connectivity (ODBC) bridge – provides JDBC access via most ODBC drivers. Some ODBC binary code and, in many cases, database client code must be loaded on each client machine that uses this driver.
- Native-API, partly Java driver – converts JDBC calls into calls on the client API for Oracle, Sybase, Informix, DB2, and other DBMSs. Like the bridge driver, this style of driver requires that some binary code be loaded on each client machine.
- Net protocol, all-Java driver – translates JDBC calls into a DBMS-independent net protocol, which is then translated into a DBMS protocol by a server. This net server middleware can connect all its Java clients to many different databases. The specific protocol used depends on the vendor. In general, this JDBC alternative is the most flexible.
- Native-protocol, all-Java driver – directly converts JDBC calls into the network protocol used by DBMSs, thus allowing a direct call from the client machine to the DBMS server. Since many of these protocols are proprietary, the database vendors themselves will be the primary source for this style of driver.

Best Practices

For applications (developed or purchased), use standards-based APIs for database access. When choosing end-user database middleware, consider products that support an SQL or universal gateway.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Point-to-point gateways APPC-only gateways	ISO RDA TOG RDA TOG SQL CU	ISO RDA TOG RDA TOG SQL CU	ISO RDA TOG RDA TOG SQL CU	ISO RDA TOG RDA TOG SQL CU	JBDC
Activities, Platforms, Operational Environments		Data Base Developers			

Table 8-20. Database access

- Microsoft's ODBC and Borland's Integrated Database API (IDAPI) are based on TOG SQL Call Level Interface (CLI).

8.4.4.4 Document Management System

8.4.4.4.1 Business, Administrative, Management Documents

Document-based data, such as word processing files, spreadsheets, photographs, microfilm, microfiche, and existing paper media represent a majority of information required to be processed, maintained, and updated by Government agencies and commercial firms. Traditional hard copy methods of document management generally include some type of filing system with hard copy or electronic indexes to facilitate retrieval of the documents. Electronic document management systems emulate the hard copy paradigms, however, many advantages can be derived, using the power of computing technology. These advantages include quick search and retrieval of documents, easy manipulation of data, rapid dissemination and routing of documents, saving of storage space, etc. With all the advantages of electronic handling of information, comes the challenge of version control. A good electronic document management system will combine the advantages that computer technology gives us with the capability to control revisions. Specifically, a document management system should include the following basic capabilities:

- Data Capture. A document management system must have the capability to capture data, either paper-based information, native electronic (e.g. Microsoft Word files), audio/video formats etc. for inclusion into the system. This data capture should also include, where possible, non-standard file formats (e.g. Adobe Acrobat).
- Data Distribution. All data within the management system should have the capability to be distributed via local/wide area networks.
- Document Manipulation. Users must have the capability to index and categorize documents, track document access/retrieval to automate business practices.
- Data Access. Rights to information with the document management system must be assigned for individual/groups of users to ensure appropriate access is granted.
- Data Retrieval. There should be the capability to deliver documents to the desktop for display, review, annotation, revision, printing, copying, faxing, e-mailing etc.
- Data Storage. A document management system should have the capability to store data both on-line, near-line, and off-site for disaster recovery purposes. Storage media should include CD-ROM, hard dives (e.g. RAID), optical disks, magnetic tape etc. as available options.
- Document Interaction with Third Party Software. To the greatest extent possible, document management systems should allow the use of third party software for extraction of data in its native format.
- Data Revision Control. All revisions to a document should be distinguished from one another. It may also be controlled through data access rights by a central group or administrator.
- Work Flow. Document management should include workflow (the capability to manage/route/create documents electronically). Significant work flow features include:
    - Information Assembly. A variety of data types can be supported.
    - Work Routing. Work routing defines the order in which the items flow.
    - Workflow Map. Work may be routed graphically without third party programming.
    - Tracking. Once implemented, the status of all transactions can be checked.

8.4.4.4.2 Technical Manuals

Navy technical manuals (TMs) and related technical text documents and training manuals concerned with weapon system and platform logistics and life cycle support require additional document management considerations. These documents will be delivered, maintained, and managed in Standard Generalized Markup Language (SGML) format in compliance with MIL-PRF-28001. TM document management systems must maintain and track many TM versions supporting corrections, engineering change revisions, and various product configurations. The document management system must support the basic capabilities outlined above for business documents, authoring and revision in an SGML environment, and document version and revision control. These management systems must address documents at a level lower than files or documents, it must support document tagging at the component level for effective product configuration management. In addition to these capabilities listed in Sec 8.4.4.4.1, TM document management systems must have the following additional capabilities:

- Collaborative Authoring and Editing. Allows one author to edit a part of a document while others edit other parts of the document.
- SGML compliant. Supports and manages SGML documents.
- Data Reuse. Allows data to be copied or shared among documents.
- Data Query. Enables data search.
- Component level management. Manages and controls edits, revisions and versioning at the document level and the SGML element/component level.
- Component version management. Manages, tracks, and indexes revision/version levels at document component (SGML element) level.
- Eliminate data redundancy. Stores, retains, and manages only one copy of document elements that appear in multiple versions of the document. This is required so that a single edit action is reflected in all versions.

Best Practices

Employ commercially available document management systems that are ODBC compliant, accept a wide variety of file formats, and allow graphical work flow routing without requiring a third party programmer. For technical manuals, the document management system must support SGML element level versioning and document management.

Guidance

Choose a document management system that will provide the following features:

- COTS available
- Visual work flow programming
- Object Oriented
- OCR/Fax/E-mail/COLD Capable
- Use CCITT GroupIV Compression Methods
- Electronic Import/Export Utility
- Interface with Third Party Programs
- Support both structured/ad hoc work flow

- OLE Compliant
- Easy to Use
- ODBC Compliant
- Network Secure
- Annotation of Data (e.g. redlines etc.)
- Multiple Output Formats (e.g. CD-ROM etc.)

For Technical Manuals:

MIL-PRF-28001 (SGML)

8.5 Data Quality and Interoperability Metrics

Chapter 10 discusses Information Quality. This section addresses measuring quality of the data from which information is derived. It defines the relationship of data metrics to information quality, describes related efforts, and identifies a process for defining a viable data metrics effort and related automated tools as part of an overall information evaluation effort.

8.5.1 Data Quality versus Information Quality

While information quality and data quality are obviously related, there are significant differences in how they are defined, measured, and achieved. Data is distinguishable from the software and refers to the information building blocks inside the computer; the data quality refers to the quality of the data within the computer databases. Information quality is the external quality that relates to the utility of computer outputs.

Drawing distinctions between software and data is difficult in database applications where data can be mistaken for a special form of software and subject to software metrics and solutions. The principal distinction is that data represents discrete pieces of raw material in the form of specially formatted real-world facts while software consists of computer program instructions for processing the data. If the raw material is incomplete, ambiguous, or otherwise flawed, then no amount of processing will produce valid information. If data is corrupt within a system, the data in a network of such systems will become geometrically more corrupt with the addition of each new source of bad data.

8.5.2 Data Interoperability

There is a requirement to develop data metrics to assess and support system data interoperability. This has been difficult because data structures are hidden in software applications and systems documentation is often inadequate or not in a common format to support analysis. As automated CASE tools are required for efficient systems development, automated performance tools are required to support data interoperability comparisons and assessments. Major database management system producers and third party vendors offer a wide range of database monitoring software with an array of metrics. For example, a major manufacturer has an integrated set of tools to measure hundreds of metrics and to provide database management performance. While these tools provide a means to measure individual database or network performance, there is still no comprehensive method of evaluating the structure and integrity of the information architecture and its data infrastructure.

The C4ISR Core Architecture Data Model (CADM), sponsored by OSD and JCS, provides a foundation for addressing the tactical information architecture. Registration of unclassified databases in the DDDS is accomplished through the Personal Computer Access Tool (PCAT). The Secure Intelligence Data Repository (SIDR) is the repository for classified databases. In addition, the Data Analysis and Reconciliation Tool (DART), produced under the aegis of the Naval Warfare Tactical Database (NWTDB), provides automated comparison of databases and message standards to assess interoperability. These tools are discussed in greater detail in Information Engineering Tools, Section 8.6.

8.5.3 Database Assessment Areas

Data is collected and stored in automated systems using a database schema. This schema may be a flat file (like a spreadsheet), a relational database or object-based system. Regardless of the schema, the areas for assessing the value of a database, and the value of the data within the database are the same. A list of questions to aid in assessment are as follows:

- Does the database contain the data required to support decision-makers at the level of their decision? This question addresses the aspects of accuracy, precision, currency, and completeness of the data. It also addresses the question of how much detail is needed for a decision at a given operational level. These quality issues are addressed in Chapter 10.
- Is there duplication within the database? Efficiency for a database means one fact in one place. Depending on the schema, replication of data within a database can either create the need for additional lines of code and hence additional costs, or cause the need for cross checking data updates to ensure all data elements are current. Such cross checking increases the costs of database maintenance. Duplication is addressed in Chapter 10.
- Is the data interoperable with other applications within a networked system? This question deals with both the format of the data and its domain. For example, data in a proprietary format may not be assessable by another application. In a similar manner, data with a domain value of degrees (true) will need a conversion for interoperability with an application that uses degrees (relative). In the first example, the data has no value to other applications regardless of its accuracy, precision, currency or completeness because it cannot be assessed. In the second example, there is a cost in converting the data to another domain value, and if the domain values are not understood to be different, then serious operational errors can occur.
- Is the data interoperable with other systems outside the network? This question not only addresses the format and domain value of a discrete data element, but also addresses the ability to tailor the data appearance from a very detailed to a less detailed view. For example, consider a radar frequency intercept by a system with accuracy to five decimal places vis-a-vis one that only stores frequencies to two decimal places. Inability to tailor the data to a useful view both for the consumer and for the automated system renders the data useless.

8.5.4 Selecting Performance Metrics

The services performed by the database could be listed as outcomes for each service request made of the system. Generally, these outcomes can be classified into three categories. The system can perform the service correctly, incorrectly, or refuse to perform the service. If the system performs the service correctly, its performance is measured by the time taken, the rate, and the resources consumed (responsiveness, productivity, and utilization metrics respectively). If the system performs the service incorrectly, an error is said to have occurred. It is helpful to classify errors and to determine the occurrences of each class of errors. If the system does not perform the

service, it is said to be down, failed, or unavailable. It is helpful to classify the failure modes and to determine the occurrences of each class.

Validity and reliability are the two most important criteria of measurement quality. Validity refers to whether the metric really measures what it is intended to measure. Reliability refers to the consistency of measurements of the metric and measurement method. Basic measures such as ratio, proportion, percentage, and rate all have specific purposes.

Desirable properties of metrics; they should:

- Be robust (that is, repeatable, precise, insensitive to minor changes)
- Suggest a norm
- Relate to specific processes, databases, or messages
- Suggest an improvement strategy
- Be a natural result of a process, database, or message (This is especially important for conserving resources when collecting metrics.)
- Be simple (and easy to explain)
- Be predictable and trackable (This allows predictions to be compared with actual experience.)

To assess interoperability of data, System Managers will document their databases in DoD approved format and produce and maintain a Data Element Dictionary and Database Structures (relationships).

The OSD developed tool to measure Levels of Systems Interoperability (LISI) should be used as guidance in determining interoperability. The LISI model is shown in Table 8-17. This tool tracks the compliance levels of the DII/COE and should be used as guidance in determining interoperability for system databases.

	Procedures	**Applications**	**Infrastructure**	**Data**
Enterprise	Enterprise Level	Interactive	Multiple Topologies	Enterprise Model
Domain	Domain Level	Groupware	World Wide Networks	Domain Model
Functional	Program Level	Desktop Automation	Local Networks	Program Model
Connected	Local/Site Level	Standard System Drivers	Simple Connection	Local
Isolated	Access Control	N/A	Independent	Private

Table 8-17. LISI Reference Model

The following describes the Data Architecture at each LISI Level:

- Enterprise (LISI Level 4) - Enterprise data models support the integration of applications. There is common understanding of the data across the enterprise.
- Domain (LISI Level 3) - Defined data models exist and are understood between applications, however, they only represent a particular domain.
- Functional (LISI Level 2) - Advanced data structures may exist but they still primarily support individual applications. Increasing commonality of data formats across programs.
- Connected (LISI Level 1) - Local data models exist, but are usually specific to a particular program.
- Isolated (LISI Level 0) - Private data models only.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DII/COE TAFIM/JTA	Imp Plans			
Activities, Platforms, Operational Environments		Data Base Developers			

Table 8-21. Data Quality and Data Interoperability Perfromance Metrics Implementation

Note

Imp Plans – the SYSCOMs, PEOs, and PMs should ensure that implementation plan(s) support directives and instructions dealing with data acquisition, information management, data administration, and information interoperability.

8.6 Information Engineering Tools

Tasks associated with information engineering and data administration are supported by a variety of specialized software tools. Tools perform two essential functions. First, in automated or semi-automated form, they provide essential efficiencies required to implement integrated, interoperable systems and data for network centric warfare in joint and coalition warfare environments. Second, they serve to precisely define and enforce management policy across the broad spectrum of users in a network centric environment.

Most of the government or commercial information management tools currently available are designed to promote efficiencies within the confines of a specific organization, functional area, or methodology. Few tools cross these boundaries to link overlapping capabilities and requirements. Network centric warfare and concepts such as data mining and warehousing all require tools that support a highly integrated information environment. The broad scope required of such tools is being defined in the tactical community by initiatives such as the C4ISR Core Architecture Data Model (CADM).

While information management describes the general policy and priorities, information engineering is made up of methodologies that are predictably and scientifically implemented. Current information engineering tools are described by categories to illustrate their capabilities and relationships. The following categories of tools are discussed:

- Process Modeling Tools
- Data Modeling Tools
- Information Transfer Management Tools
- Architecture Management Tools

8.6.1 Process Modeling Tools

The standard for process modeling within the DoD is defined as the IDEF0 standard and is promulgated in Federal Information Processing Standards Publication, FIPS-183. Currently, the

most widely used commercial tool in the DoD that complies with this standard is BPwin by Logic Works, Inc. Future tools in this area should broaden their perspective and capture more specific process concepts as described in the DoD structures of the Universal Joint Task List (UJTL), service extensions to UJTL, and the C4ISR CADM. The Data Analysis and Reconciliation Tool (DART) is one the few tools which incorporates the UJTL and has a goal of incorporating components from the CADM.

8.6.2 Data Modeling Tools

A wide variety of government and commercial tools exist to support data modeling. The DoD standard for data modeling is defined as the IDEF1X standard and is promulgated in Federal Information Processing Standards Publication, FIPS-184. Among the most widely used commercial tools in the DoD that comply with this standard is ERwin by Logic Works, Inc.

- The Defense Data Dictionary System (DDDS) is the DoD core repository for defining standard and non-standard data elements. The Personal Computer Access Tool (PCAT) is a standalone, Microsoft Windows based implementation of the DDDS. While the DDDS and PCAT both focus at the data element dictionary level, they have plans to directly integrate with the IDEF1X standard in the future.
- In order to meet the requirements for managing classified data models the Secure Intelligence Data Repository (SIDR) is being developed for the intelligence community.
- The Comprehensive Utilities for Data Administration (CUDA) is a web based, client-server tool developed by the Naval Meteorology and Oceanographic Command (METOC). This tool complies with the data element standards of the DDDS and integrates this data dictionary with the IDEF1X ERwin tool. The CUDA includes capabilities for both model display in the web environment and collaborative groupware modeling.
- The DART complies with the DDDS data element registration standard, and it also integrates system modeling and extensive inter-system and information transfer standard comparison/analysis functions.

8.6.3 Information Transfer Management Tools

DoD information standards include USMTF, TADIL, and VMF along with their NATO equivalents. The integration transfer and database system standards have been a relatively recent initiative. The most prominent commercial tool is IRIS, European workstation grade tool. The most capable government tool is embodied in the Message Transfer Standard (MTF) extension to the DART. This tool examines and compares US/NATO MTF baselines both among themselves and with DART registered database systems.

8.6.4 Architecture Management Tools

Architecture management tools are those that must respond to the broad and dynamic environment of both network centric warfare and commercial enterprises such as data warehousing and data mining.

- A vision of the broad scope of such a DoD tool is suggested by developing architecture initiatives such as the C4ISR CADM. The CADM embodies and integrates many existing DoD and Services information architectures including the DoD Data Model, C2 Core Data Model, and the Navy’s C4ISR Architecture Data Model.

- One of the few tools which has begun to capture this broad perspective is the DART, as part of the Naval Warfare Tactical Database (NWTDB) initiative. The DART has an integrated agenda that includes the registration of databases as real-world systems, information transfer standards registration, and DoD data dictionary standards.

These individual perspectives can then be subjected to individual and comparative analysis by automated and semi-automated processes. However, a fully capable architecture tool would have an even broader scope that would include rapid configuration management of information interoperability over a large community of users. Extended capabilities would need to examine and validate real-world operational data in addition to system descriptions.

8.6.5 GOTS Information Tool Descriptions

Comprehensive Utilities for Data Administrators (CUDA)

This application was developed to address the needs of Data Administrators not otherwise addressed by commercial or government supplied software products. The developers of the CUDA integrated and extended it from the existing suite of software to include some emerging technologies. The CUDA provides Data Administrators with a low-cost data model-based repository for prospective and approved data standards. The provided functions include:

- Batch loading of proposed standards from ERwin to the DDDS.
- Synchronization of ERwin with the data standards/metadata contained in the DDDS.
- Production of files to support the publication of data models on the World Wide Web (WWW).

Data Analysis and Reconciliation Tool (DART)

DART is a Microsoft Windows-based application that provides the following

- Database registration and reverse engineering (capturing existing database formats and structures)
- Data standardization (data element matching, mapping, and generation)
- Database configuration management and version control
- Database integration (migration system database engineering)

DART was developed as a part of the Naval Tactical Warfare Database (NWTDB) project. The NWTDB process unites users, system developers, database producers, and data administrators to solve data interoperability problems.

Health Information Resources Service (HIRS)

HIRS is an advanced form of repository in support of the DoD Health Affairs community. Traditionally, a repository contains a knowledge base of information about the organization, its goals, entities, records, organizational units, functional processes, procedures, applications and information systems. HIRS provides these services, but also provides an integrating technology that enables users to access information from a variety of sources. These facilities are provided within the HIRS Virtual Environment independent of which organization information systems are automated and the mix of automation technologies employed. HIRS is freely accessible on the WWW, however, the virtual library provides configuration management type access controls and certain parts of HIRS are password controlled.

The HIRS Standard Model Warehouse is an ISO-PCTE compliant standards-based tool set. The standard CASE tool methodologies of IDEF, CDIF, and OMT are integrated into a common repository. This architecture allows for CASE tool translation, migration to other methodologies (such as from IDEF1X data modeling to Object Modeling Technique) mapping/matching, and integration of multiple models in various tools (including IE:Advantage, ERwin, BPwin, AI0win, Rational Rose, Paradigm Plus, Object Maker, OM Tool), and configuration/model management tools.

Marine Air-Ground Task Force (MAGTF) Data Library/Data Dictionary System (MDL/DDS)

A non-proprietary MS Windows-based tool, the MDL/DDS is used to automate quality specifications and perform data set validations prior to distributing reference data on CD-ROM. The Data Quality Engineering (DQE) tool set has been created from COTS combined with C++ code. A combination of WATCOM (COTS) database and CASE tools are used to automate the data standardization, data mapping/matching, and domain specification processes.

The tool is divided into two major applications with discrete, but interrelated sub-functions called workbenches. The DQE application provides the necessary functions to perform database management and data quality engineering. The DDS application provides data administration functions such as data standardization, mapping/matching, and metadata repository. The DQE Workbench evaluates incoming and outgoing reference data, using a custom procedure editor for creating User-Defined Rules (UDRs) and performing special queries. This automated tool assists with the generation of SQL script. A report utility enhances raw query output with graphs, filters, and text processing options.

The DDS supports DoD compliant data standardization, and holds all required and optional metadata as prescribed in DoD 8320 guidelines. It can be modified to support any set of guidelines. The DDS Workbench performs data standardization functions that include a query by example, filter, search, insert, standard name and access mnemonic generation features. The mapping element option is consistent with the DoD guidelines. This module also supports direct interface mapping as follows:

- Application Element to Application Element
- Application Element to Reference Dictionary Element
- Reference Dictionary Element to Application Element
- Reference Dictionary Element to Reference Dictionary Element

System Administrator support includes window level access security, user privileges, user address records, and password control.

Personal Computer Access Tool (PCAT)

PCAT version 2.1 is a stand-alone version of the Defense Data Dictionary System (DDDS). The DDDS is the primary automated tool that supports DoD Data Administration in developing and managing standard data per DoD Directive 8320.1. PCAT provides a user-friendly method for searching and analyzing all the DoD standard and non-standard data elements and primewords that reside in the DDDS. It provides a mechanism for defining metadata, cross-referencing and consistency checking, and supports the standardization of data element names, definitions, and relationships. PCAT was developed to support data analysis and data administration.

Some of the features of this tool include: list- and keyword-based searches, customized data filters, data element creation, naming convention validation, user-guided thesaurus, reports, on-line help, multi-user access, data import/export, and stand-alone or LAN server implementation. Users can download updated PCAT databases (MS Access) monthly via FTP.

Secure Intelligence Data Repository (SIDR)

The Functional Data Administrator for Intelligence (FDA-I) developed the SIDR Prototype for the DoD Intelligence Community. It is a data standardization tool that permits users with little knowledge of DoD 8320.1-M-1 data standardization procedures to consistently produce standards compliant data. The SIDR 8320 Application is also an information management analysis tool that permits users to quickly research and associate standard and non-standard data to related data, models, applications, documents, and organizations. SIDR enforces compliance with DoD 8320.1-M-1, IDEF0, IDEF1X standards.

SIDR can import data from various tools and applications such as IE:Advantage, ERwin, and the DDDS. Once data has been imported into SIDR, the tool's powerful search engine assists the data analyst in creating DoD compliant standard data. The search engine performs searches against standard and nonstandard data to determine if similar data exists. The tool guides prompt the user to use DoD mandatory fields and flag any data that does not meet DoD 8320.1-M-1 requirements. SIDR also allows new versions of approved DoD elements to be created. This tool also imports non-standard data from legacy systems for researching standard data elements and for traceability. The new standards information developed can be batch loaded directly into the DDDS.

System for Model Analysis, Reporting and Tracking (SMART)

SMART was developed by HQ SSG/ENSD to support data analysis and data administration. It enforces the 8320.1-M-1 and FIPS 184 standards. This Microsoft Access-based application is integrated with Logic Works ERwin (a database design and modeling tool), Microsoft Word, and PCAT SMART can be implemented as a stand-alone or on a LAN server.

Some of the features of the SMART tool include: standard data element creation, data element and model standards compliance validation, integration of model and metadata information, data standardization submission package generation, package archival and tracking, and application of DISA notation to model objects. SMART supports DDDS import/export formats and Microsoft Access MDB file format. It was developed to support the requirements of data analysis and data administration, and adheres to DoD Directive 8320.1, DoD Data Administration, and Federal Information Processing Standards (FIPS) Publication 184, "Specifications for Integration Definition for Information Modeling (IDEF1X)".

Best Practices

Government and commercial tools should be selected based on their inherent utility, compliance with standing directives, and level of acceptance within the DoD community.

Guidelines and priorities should be set for the use of tools in support of specific information management requirements and needs. The dynamics of the tool environment are characterized by active inputs to tool development and continuing update of tool selection guidelines.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	GOTS with COTS Support	Imp Plans	Updates	Updates	COTS with GOTS Support
Activities, Platforms, Operational Environments		Data Base Developers			

Table 8-14. Information Engineering Tool Implementation

8.7 References

Booch, Grady, Object-Oriented Analysis and Design with Applications, Second Edition, ISBN 0-8053-5340-2, Benjamin/Cummings Publishing Company, Inc., Redwood City, California, 1994

Brown; IDEF1X Formalization, The Database Design Group, Inc., 15 November 1992 (copyrighted by DDG)

Bruce (Institute for Defense Analysis); *On IDEF1X - - The Why and How of What, A Seminar on Database Quality*, Course Notebook, 13-15 October 1992

C4I Integration Support Activity (CISA) C4ISR Integration Task Force, Integrated Architectures Panel, *C4 Architecture Framework*, Version 1.0, CISA-0000-104-96, 7 June 1996

C4ISR Integration Task Force, Integrated Architectures Panel, Integrated Architectures Panel Final Report 3 June 1996

Chief of Naval Operations; OPNAVINST 9410.6, “Naval Warfare Tactical Database (NWTDB) Requirements for Tactical Warfare Systems” of 13 July 1993

Chief of Naval Operations; OPNAVINST 3140.54A of 5 Nov 93, “Submission of Meteorologic and Oceanographic (METOC), Astrometry, and Precise Time and Time Interval (PTTI) Requirements”

Chief of Naval Operations; OPNAVINST 3140.55 of 5 Mar 87, “Submission of Requirements for Mapping, Charting, and Geodesy (MC&G) Products and Services”

Chief of Naval Operations; OPNAVINST 3430.23B of 12 Jun 92, “Tactical Electronic Warfare Reprogrammable Library Support Program”

Chief of Naval Operations; OPNAVINST 9410.5, “Interoperability and Information Requirements for Tactical Naval Warfare Systems”

Chief of Naval Operations; OPNAVINST 9410.6, of 13 July 1993, “Naval Warfare Tactical Database (NWTDB) Requirements for Tactical Warfare Systems”

Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO), *C2 Core Data Model*, Version 2.0, 1 July 1994

Defense Information Systems Agency (DISA); "Defense Information Infrastructure Common Operating Environment (DII COE);" 1 May 1998; http://spider.osfl.disa.mil/dii/ (24 May 1998)

Department of Defense(DoD*) Joint Technical Architecture*, Version 1.0, 22 August 1996, UNCLASSIFIED (Draft Version 2.0 of 26 May 1998 is available for comment through http://www-jta.itsi.disa.mil/ (30 May 1998))

Department of Defense (DOD); Technical Architecture Framework for Information Management (TAFIM), Version 3.0, 30 April 1996

Department of Defense (DOD) Directive 4630.5, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems. ASD (C3I)," 18 November 1992

Department of Defense (DOD) Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems," 18 November 1992, UNCLASSIFIED.

Deputy Under Secretary of Defense (DUSD) (Acquisition and Technology) and ASD (C3I), Memorandum to Joint Chiefs of Staff, Office of the Secretary of Defense, and Military Departments and Agencies, "Department of Defense (DOD) Implementation Guidance for the Joint Technical Architecture," 22 August 1996

Department of Defense (DOD) Directive 5000.1, "Defense Acquisition", 15 March 1996

Department of Defense (DOD) Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems", 15 March 1996 [Replaces DoD Directive 8120.1 and 8120.2]

Department of Defense (DOD) Directive 8000.1, "Defense Information Management (IM) Program, ASD (C3I)", 27 October 1992

Department of Defense (DOD) Directive 8320.1, "DoD Data Administration", 26 September 1991

Department of Defense (DOD) 8320.1-M, "DOD Data Administration Procedures", March 1994

Department of Defense (DOD) 8320.1-M-1, "DOD Data Element Standardization Procedures" February 1998 (Draft)

Department of Defense (DOD) "Information Technology Management (18M) Strategic Plan," Version 1.0, March 1997

Information Technology Management Reform Act of 1996 (ITMRA 96), Public Law 104-106, (Also known as the "Clinger-Cohen Act.")
http://www.dtic.mil/c3i/cio/references/itmra/itmra.Annot.html (24 May 1998)

Joint Staff, Joint Publication Number 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Includes US Acronyms and Abbreviations and NATO Terms (English Only)), 23 March 1994

Joint Staff; "Universal Task List" (UTL) Version 3.0; 13 September 1997

Kientzle, Internet File Formats; Coriolis Group Inc; Scottsdale, AZ 1995

National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 183 "Integration Definition for Function Modeling (IDEF0), 21 December 1993; http://www.dtic.mil/c3i/bprcd/484t.htm (30 May 1998)

Navy Intelligence Command; NAVINTCOMINST 3890.1C, "Intelligence Production Tasking Procedures" of 12 Jul 89

Space and Naval Warfare Systems Command (SPAWAR) Deputy Chief Engineer for Architecture and Standards and the Naval Architecture Working Group (NAWG), Operational and Systems Architecture Division (SPAWAR 051-2), "Naval C4ISR Architecture Primer," 17 January 1997

9. Applications

This chapter includes the standards guidance for the software components that support specific operational and business functions. The relationship of this chapter with the ITSG is shown in Figure 9-1.

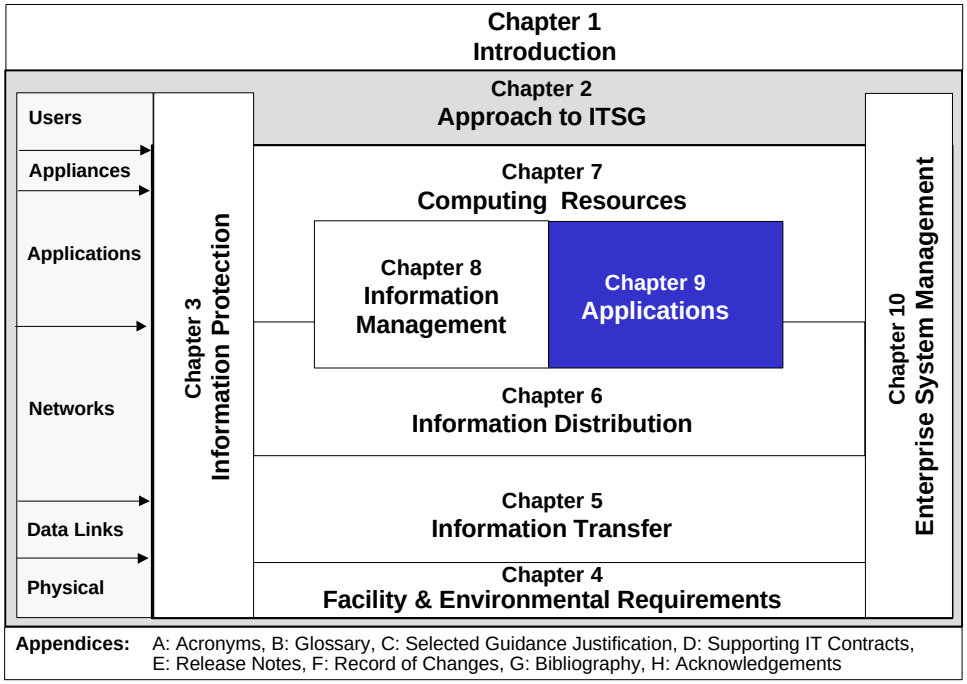


Figure 9-1. ITSG Document Map highlighting Chapter 9, Applications

9.1 Overview

9.1.1 Background

Applications consist of hardware and software components that support specific operational and business functions, including C4ISR systems that allow the warfighter to selectively pull in timely targeting information, the navigator to display cartographic information, and for the logistician to locate a critical spare part necessary to complete a mission. They include the common tools by which people across the Navy and Marine Corps prepare text documents, analyze daily activities, develop and present mission briefings, and make decisions. Applications are the myriad of tools by which the DON leverages IT to support its improved processes and thereby realizes large order of magnitude gains in information superiority and worker productivity with commensurate reductions in cost.

Applications are dependent upon an enterprise architecture and standards for integration, effectiveness and interoperability. The operational architecture defines the requirements, conditions and performance levels for information exchange. The systems architecture identifies the specific applications that perform the mission tasks and business functions — where those applications reside, who controls them, what systems they interoperate with, and who accesses them.

An application is a user's agent to do the required work within the information infrastructure. Chapter 8 describes "information" as the payload of the infrastructure, and Chapter 6 describes the 'envelope' for the data (e.g., MIME types). "Applications" comprise the factory that processes the payload to turn out the final product — operational capability. Applications transform information and produce a capability to better understand the situation, make better decisions, issue clear direction, create and promulgate new information, and allow people to communicate.

The ITSG document map, Figure 9-1, depicts applications and information at the core of information technology and they are surrounded by computing resources and information distribution technologies. This illustrates the role applications play in processing information using the computer resources and disseminating the resultant products to the user via a human computer interface of the information distribution network. Figure 9-2 shows the relationship of applications to the information infrastructure using a modified form of the DOD Technical Reference Model.

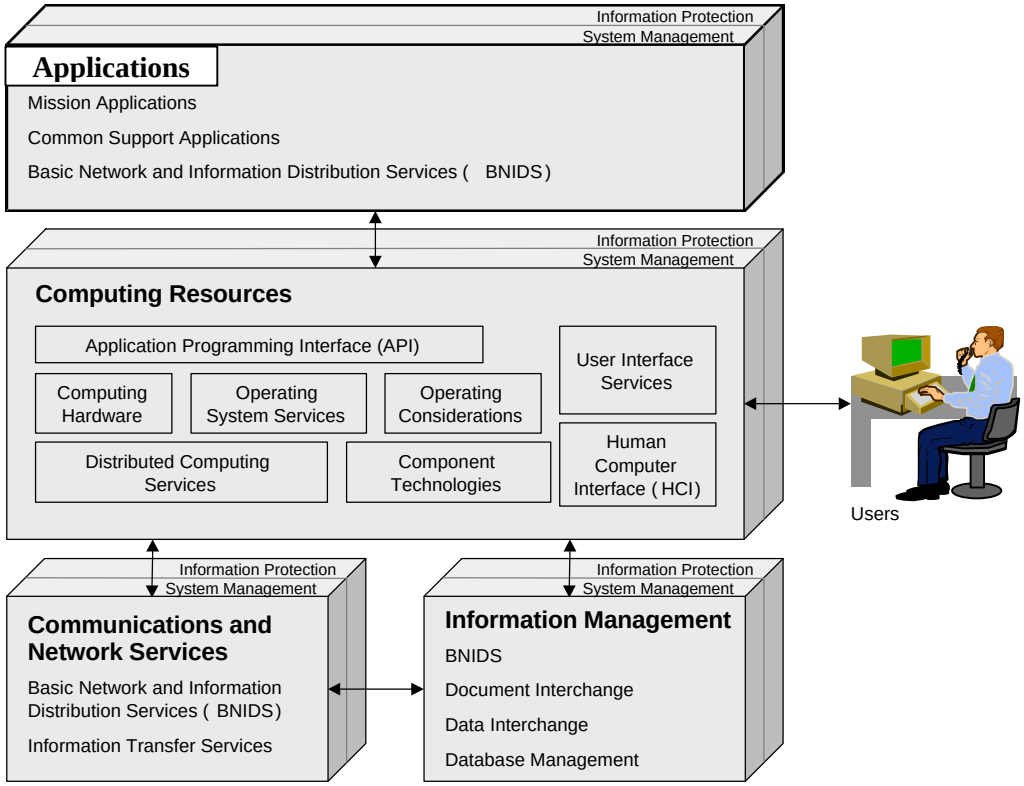


Figure 9-2. Applications in the Context of the DOD Technical Reference Model

Figure 9-2 shows the applications box that includes mission applications, common support applications and the Basic Network and Information Distribution Services (BNIDS). All of these elements consider information protection and system management. BNIDS provides basic fundamental capability to all applications and operators to connect and integrate the user with application servers, data servers, and other application subscribers. Common support applications provide capabilities to support functions common to all users above those provided in BNIDS. These applications include basic office automation functions such as word processing and database access. They also include advanced communication services such as integrated telephony, video teleconferencing and distributed collaborative planning.

- From an information technology viewpoint, applications are collections of system components that support a particular task or function. They include end-to-end, multi-media communications as well as information management and decision support capability. Applications can be self-contained and reside locally on a user's personal workstations, or they can be a system of distributed computers integrated to perform a function. Distributed computing applications require a three-tiered architecture involving: (1) application server, (2) data server, (3) presentation clients, all connected by the network (Figure 9-3) (or contained within the same computer). Communication applications normally involve a minimum of two communication devices connected by the network.

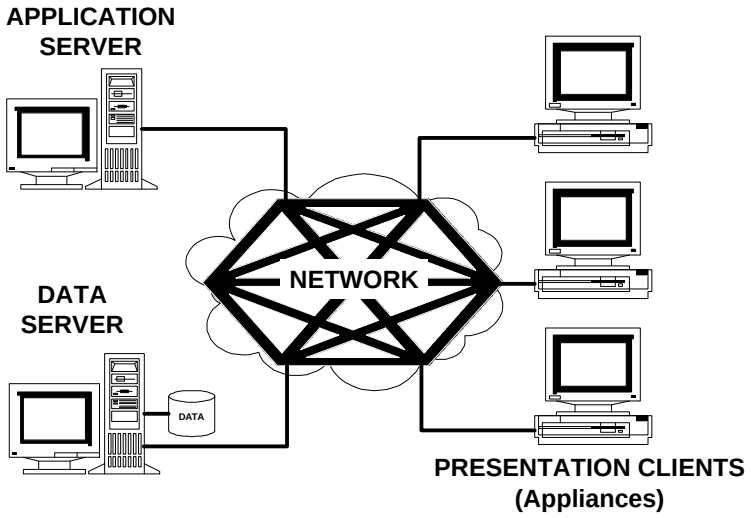


Figure 9-3. Three-Tiered Application Architecture

9.1.2 Defense Information Infrastructure Common Operating Environment (DII COE)

The Defense Information Infrastructure (DII) Common Operating Environment (COE) is a collection of reusable software components; it is a software infrastructure for supporting mission-area applications, guidelines, standards and specifications. The DII COE Integration and Runtime Specification (I&RTS), CM-400-01-03, dated 1 January 1997, outlines these guidelines and rules. It describes how to reuse existing software and properly build new software so that integration is seamless and extensively automated. The DII COE defines eight progressively deeper levels of integration for the runtime environment. These levels are directly tied to the degree of interoperability achieved. The I&RTS document is the result of collaboration among the Services, the Joint Staff , USD(A&T), ASD (C3I), DISA, DIA and other elements of the intelligence community.[12] Software implementation within the DON will be in compliance with the DII COE.

The DII COE is based on the DOD Technical Reference Model (TRM) layered architecture that defines the services and interfaces that are common to all information processing systems[13]. The top layer of the TRM depicts the mission area applications (e.g., command and control, logistics) that are focused on specific functional requirements. The second layer includes common support

[12] This paragraph is taken verbatim from Assistant Secretary of Defense letter of 2 May 1997; Subject: *Implementation of Defense Information Infrastructure Common Operating Environment Compliance*

[13] The TRM is depicted in figure 2-17 and discussed in section 2.11.2. A modified version of the TRM is provided as figure 9-2.

applications; those support the mission area applications and provide services necessary to view data in a common way. The top two layers are referred to as the application software entity and include all DOD application software. The mission area applications at layer one of the TRM are integrated into DII COE by means of a common set of Application Program Interfaces (APIs).

Applications fall into several categories – Commercial Off-The-Shelf (COTS), Government-Off-The-Shelf (GOTS), custom-developed, or a combination based upon the need to "customize" COTS or GOTS software to better support the mission requirement. Regardless of the software origin, interoperability can be achieved through consistent use of agreed-upon standards. The DII COE contains a list of both COTS and GOTS software that meets DOD interoperability requirements.

9.1.3 Beyond Software

Applications go beyond distributed software programs – they include all methods by which the user controls the information infrastructure to attain an operational or support capability. Applications in this context also include hardware or combined hardware and software systems that control, manage or transfer information. This expands the scope of applications from software programs to computer telephony, video teleconferencing (VTC), and video on demand (VOD).

9.1.4 Outline

The policy, standards and guidance that are provided in this chapter define how the applications interrelate with themselves and with the user. The grouping of specific application standards is provided to collectively address the common operating environment for applications across the DON. The topics below provide a logical approach to dealing with information technology standards as they relate to warfare and warfare support functions of the operational and functional support commands. Many of these will be combined for applications such as distributed collaborative planning and outreach education/training.

Common Support Applications – Office automation, multimedia, interpersonal communications, environment management, database utilities, graphics and imagery, and engineering support

Cooperative Work Applications – Electronic forms, workflow management, conferencing, calendaring and scheduling, and decision support

Computer Telephony – Computer intelligence for telephone supported data transactions

Video Teleconferencing – Video conferencing services for geographically dispersed activities

Mission Applications – Enterprise functional systems

Application Support Services – System (hardware and software) engineering and maintenance services

9.2 Common Support Applications

Support applications are common applications (e.g., word processing, spreadsheets) beyond BNIDS that can be standardized across individual or multiple mission areas to support enterprise wide user requirements. Support applications can provide a mission-specific service or they can provide general service. The DON policy is to use COTS products. GOTS applications may be required to meet a DON-unique need and reused in multiple information systems. It is expected that GOTS will only be required to meet mission specific applications.

Support applications also include cooperative work applications such as electronic forms, workflow management, conferencing, calendaring and scheduling, and group decision support.

9.2.1 Office Automation

Office automation services provide common office functions used in day-to-day business operations. Office automation support services include:

Word Processing Services – Creating, editing, formatting and manipulating text documents including the insertion of multimedia objects (Section 9.2.2). Includes electronic and hard-copy production.

Briefing and Presentation Services – Creating, editing, formatting, manipulating and displaying slides and handouts for presentations. Includes the insertion and manipulation of multimedia objects (Section 9.2.2).

Spreadsheet Service – Creating, calculating, manipulating and presenting information in tables or charts. This capability should include fourth-generation-language-like capabilities that enable the use of programming logic within spreadsheets.

Project Management Services - Tools that support the planning, administration, and management of projects.

Calculation Services - Including the capability to perform routine and complex arithmetic calculations.

Office Suite. Assembling each of the above services in a tightly integrated suite that maximizes ease of information content and format transfer from one application to another to maximize final product effectiveness. Includes electronic document management to allow indexing, storage and retrieval of information products.

Best Practices

Choose a commercial product that best suites the organization's needs. This choice can be emotional because it often involves a conflict between a product that many people are familiar with at home or from previous work experience, and the product that is best for the enterprise. The products should provide enterprise information interoperability as well as working set efficiency as discussed in Section 2.1.3. It should foster easy sharing and processing of information objects (text, graphics, etc.) within the organization, community of interest, and the entire DON enterprise. The product should be compatible with groupware products discussed in Section 9.3.

Recommended Implementation

Not determined at this time.

9.2.2 Multimedia Information Processing

Multimedia services provide the capability to manipulate and manage information consisting of text, graphics, images, video, and audio. These services can be used directly by mission area applications, but they can also be used by other support applications to satisfy a common requirement. Multimedia services include:

Document processing services, including the capability to create, edit, merge, and format documents. These services enable the composition of documents that incorporate graphics, images, and even voice annotation, along with stylized text. Included are advanced formatting and editing services such as style guides, spell checking, use of multiple columns, table of contents generation, headers and footers, and outlining tools.

Electronic publishing services, including incorporation of photographic quality images and color graphics, and advanced formatting and style features such as wrapping text around graphic objects or pictures and kerning (i.e., changing the spacing between text characters). These services also interface with sophisticated printing and production equipment.

Geographic Information System (GIS) services, including the capability to create, combine, manipulate, analyze, and present geospatial (including cartography) information. This includes the creation of entity symbology that overlays the map background display and access to standard symbol libraries.

Image processing services providing for the capture, scan, creation, and edit of images in accordance with recognized image formatting standards.

Video processing services, including the capability to capture, compose, and edit video information. Still graphics and title generation services are also provided.

Audio processing services, including the capability to capture, compose, and edit audio information.

Multimedia processing services, including the capability to compress, store, retrieve, modify, sort, search, and print all or any combination of the above-mentioned media, and to perform these actions on two or more types of media simultaneously. This includes support for microform media, optical storage technology that allows for storage of scanned or computer produced documents using digital storage techniques, a scanning capability, and data compression. Additionally, multimedia processing includes hypermedia processing. Hypermedia provides the capability to create and browse documents that allow users to interactively navigate through the document using information embedded in the document.

Best Practices

Use standard commercial products for multi-media information processing.

Recommended Implementation

Not determined at this time.

9.2.3 Interpersonal Communications

Interpersonal communications services provide the capability to send, receive, forward, and manage electronic and voice messages. They also provide real-time information exchange services in support of interpersonal conferences. Additional information on electronic messaging interface standards can be found in Section 6.2.1.

Standard messaging APIs provide access to directory services, message store-and-forward capabilities, and electronic transport capabilities of e-mail message handling systems. A message type called X.435, present in the 1988 version of X.400, provides standardized support for Electronic Data Interchange (EDI) transaction transport and interchange over communications networks. This EDI message type facilitates the movement, delivery, and security of EDI transactions over X.400 networks.

An e-mail message handling system's message store-and-forward and electronic transport capabilities can be accessed by applications through the APIs listed in Table 9-1.

Best Practices

Use standard commercial products for interpersonal communications.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
VIM	CMC/2 Extended MAPI	CMC/2 Extended MAPI	CMC/2 Extended MAPI	CMC/2 Extended MAPI	VIC
Activities, Platforms, Operational Environments		Application Developers			

Table 9-1. Data delivery: application programming interfaces

- The Vendor-Independent Messaging (VIM) interface is supported by Apple, Borland, IBM, Lotus, and Novell. Several of these suppliers are now supporting MAPI as well as VIM. Avoid using VIM because it is not widely accepted.
- The Common Messaging Call (CMC) API standard, developed by the X.400 API Association (XAPIA) in conjunction with the Electronic Mail Association (EMA), addresses compatibility issues when users write message-enabled applications. XAPIA, an international standards group of the ITU-T, is working on specifications for the basic functions of sending and receiving e-mail messages. These specifications are based heavily on Messaging Application Programming Interface (MAPI) specifications.
- APIs are being developed to address the issues of seamlessly exchanging scheduling and calendaring data. Most efforts are, however, still proprietary. One such API, Vendor-Independent Calendaring (VIC), is being developed by the Lotus Consortium and the EMA.
- MAPI is supported by Digital, Hewlett-Packard Co. (HP), Microsoft, Oracle Corp., Lotus, and Novell.
- Open Collaboration Environment (OCE), developed for the Macintosh platform by Apple, is designed to support VIM and MAPI.

9.2.4 Environment Management

This type of service is broader in scope than the other categories in that it exists primarily to manage a particular data processing and/or communications environment. Environment management services integrate and manage the execution of platform services for particular applications and users. These services are invoked via an easy-to-use, high-level interface that enables users and applications to invoke platform services without having to know the details of the technical environment. The environment management service determines which platform service is used to satisfy the request and manages access to it through the API. These services include:

Batch processing services support the capability to queue work (jobs) and manage the sequencing of processing based on job control commands and lists of data. These services also include support for the management of the output of batch processing, which frequently includes updated files or databases and information products such as printed reports or electronic documents. Batch processing is performed asynchronously from the user requesting the job.

Transaction processing services provide support for the on-line capture and processing of information in an interactive exchange with the user. This typically involves predetermined sequences of data entry, validation, display, and update or inquiry against a file or database. It also includes services to prioritize and track transactions. Transaction processing services may include support for distribution of transactions to a combination of local and remote processors.

Information presentation and distribution services are used to manage the distribution and presentation of information from batch and interactive applications. These services are used to shield mission-area applications from how information is used. They allow mission area applications to create generic pools of information without embedding controls that dictate the use of that information. Information distribution and presentation services include the selection of the appropriate formatting services required to accomplish the distribution and presentation of information to a variety of mission-area applications, support applications, and users. It also includes the capability to store, archive, prioritize, restrict, and recreate information.

Computer-based training services provide for an integrated training environment on user workstations. Training is available on an as-needed basis for any application available in the environment. Electronic notes are provided at the stroke of a key from anywhere within the application. This includes tutorial training on the application in use and the availability of off-line, on-site interactive training. The DoD on-line training environment will provide in-depth training to the new user, guidance to the novice user, and refresher material for the more experienced user. Computer-based training includes on-line documentation services. As a system service, generalized help files that have index, contents, and context-sensitive definitions must be added to all applications. The goal is for a user, through a system-managed activity, to be able to obtain help at any point, while on line.

Best Practices

Use standard commercial products for computing environment management.

Recommended Implementation

Not determined at this time.

9.2.5 Database Utilities

Database utility services provide the capability to retrieve, organize, and manipulate data extracted from a database management system. These common services provide a consistent interface to the user while providing access to a variety of databases. Database utility services include:

Query processing services that provide for interactive selection, extraction, and formatting of stored information from files and databases. Query processing services are invoked via user-oriented languages and tools (often referred to as fourth-generation languages), which simplify the definition of searching criteria and aid in creating effective presentation of the retrieved information (including use of graphics). Fourth-generation languages are generally proprietary. As yet, no public domain fourth-generation language is in wide business use.

Screen generation services that provide the capability to define and generate screens that support the retrieval, presentation, and update of data.

Report generation services that provide the capability to define and generate hardcopy reports composed of data extracted from a database.

Networking/concurrent access services that manage concurrent user access to database management system (DBMS) services.

Best Practices

Use standard commercial products for data base utilities.

Recommended Implementation

Not determined at this time.

9.2.6 Graphics and Imaging

Graphics and imaging applications provide functions required for creating, storing, retrieving, and manipulating images. These functions include services such as graphical object management, drawing services, and imaging functions.

9.2.6.1 Imaging Systems

Imaging systems have the potential to reduce the number of paper documents in an organization. Most imaging systems provide scanning, optical character recognition (OCR), indexing, storage, and retrieval components. Users may then search for content, retrieve documents, annotate (or update in OCR environments), and, in some cases, route the documents over a messaging system.

The primary purpose of these systems is to convert existing paper-based information into digital images, editable forms, plain text, or compound documents. Some imaging systems have built-in

workflow capabilities, and others may be used to create the digital objects that will be fed into a stand-alone workflow management system.

Best Practices

Choose an imaging product based on its capability to support industry-adopted standards and on the Client /Server model of computing.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	NITFS MIL-STD-2500A MIL-STD-188-196 MIL-STD-188-199 ANSI/ISO 8631 ISO-IEC 10981-1	NITFS MIL-STD-2500A MIL-STD-188-196 MIL-STD-188-199 ANSI/ISO 8631 ISO-IEC 10981-1	NITFS MIL-STD-2500A MIL-STD-188-196 MIL-STD-188-199 ANSI/ISO 8631 ISO-IEC 10981-1	NITFS MIL-STD-2500A MIL-STD-188-196 MIL-STD-188-199 ANSI/ISO 8631 ISO-IEC 10981-1	
Activities, Platforms, Operational Environments		Application Developers			

Table 9-2. Data delivery: application programming interfaces

- NITFS provides a package containing information about the image, the image itself, and optional overlay graphics. It was developed and mandated by ASD C3I for dissemination of digital imagery from overhead collection platforms. Guidance on applying the suite of standards can be found in MIL-HDBK-1300A. The following standards are mandated for secondary imagery dissemination:
- MIL-STD-2500A, National Imagery Transmission Format (Version 2.0) for file format.
- MIL-STD-188-196, Bi-Level Image Compression
- MIL-STD-188-199, Vector Quantization Decompression
- ANSI/ISO 8631: 1992, Computer Graphics Metafile (CGM) as profiled by FIPS 128 and MIL-STD-2301
- ISO-IEC 10918-1: 1994, Joint Photographic Experts Group (JPEG) as profiled by MIL-STD-188-198A. Although the NITFS uses the same ISO JPEG algorithm as mandated in Section 2.2.2.2.1.4.2, the NITFS file format is not interchangeable with the JFIF file format.

9.2.6.2 Three-Dimensional Computer Graphics

OpenGL is a mature standard in the engineering and business application environment. Other 3-D APIs, such as Open Inventor, support slightly different goals.

Best Practices

For new development, select OpenGL API set.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
GKS-3-D	OpenGL	OpenGL	OpenGL	OpenGL	Open Inventor
Activities, Platforms, Operational Environments					

Table 9-3 3-D Computer Graphics

9.2.7 Engineering Support

Engineering support services include support for analysis, design, modeling, development, and simulation for a wide variety of users and environments. This includes computer-aided design services for designing, drafting, and producing engineering drawings. It also includes services provided by decision support development tools and expert system shells.

Computer-aided design (CAD) services provide high-precision drawing tools and modeling capabilities to allow production of engineering specification drawings and other precise drawings.

Decision support services provide interactive modeling and simulation tools that support analysis of alternative decisions.

Expert system services provide artificial intelligence capabilities usually based on knowledge- or rules-based inference engines that recommend or take actions based on presented situations and prior “experiences.”

Modeling and simulation services provide the capability to capture or set object characteristics or attributes and parameters of a system of objects, and to portray the relationships and interactions of the objects to assist in the analysis of the system.

Best Practices

Not determined at this time.

Recommended Implementation

Choose products available on DOD contracts. Appendix D provides information on Navy contracts.

9.3 Cooperative Work Applications

Cooperative work applications, or workgroup computing, or groupware, takes advantage of personal computing and office automation by offering information sharing across the enterprise. Emerging workgroup applications, combined with technology advances, provide an environment

to allows the redesign of business processes regardless of geographic, organizational, or software boundaries.

Groupware addresses the need to facilitate and improve the unstructured communication processes of the organization. These applications include collaborative authoring, document sharing, and shared databases. The term groupware is generally defined as “computer-based systems that support groups of people engaged in a common task (or goal) and that provide an interface to a shared environment.” The groupware environment has three facets: the task or business process to be performed, the time in which individuals participate, and the location of each individual. The design point for groupware is to accomplish the business process in the most efficient manner possible by eliminating the need to work at the same place or at the same time.

Groupware tools can be categorized by functionality. The Institute for the Future originally defined the FourSquare+ model shown in Figure 9-4. The model categorizes the various forms of groupware based on the dimensions of time and place of the group interaction. The center represents the basic groupware platforms.

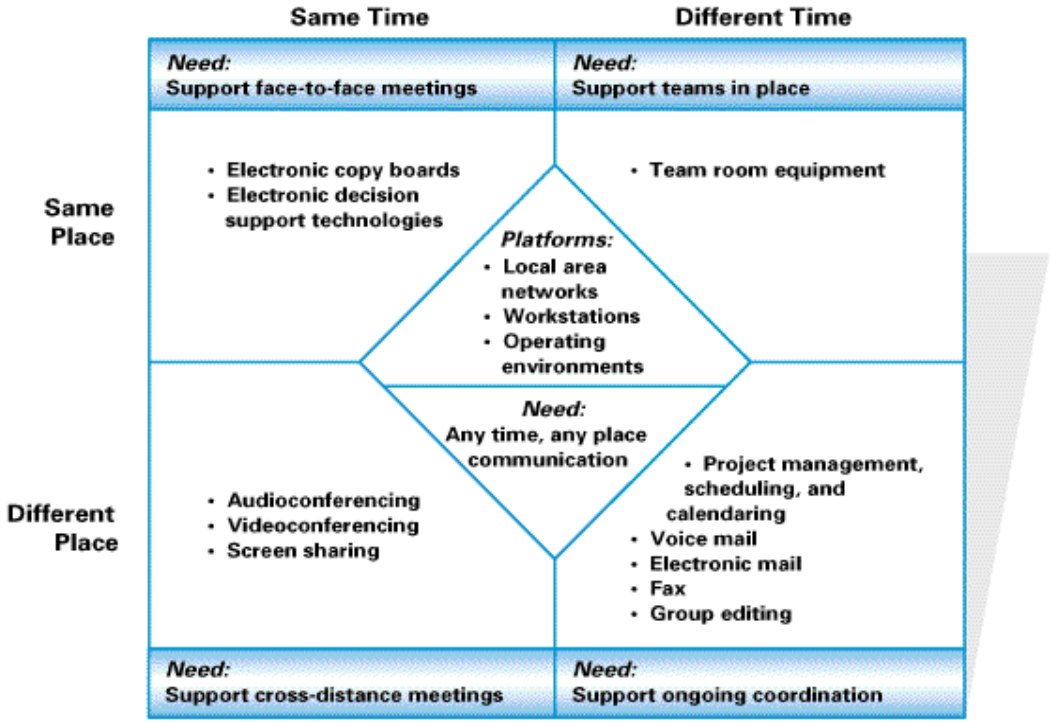


Figure 9-4. Forms of Groupware

Groupware can lead to the creation of new business data by capturing the process supported by groupware tools. The use of groupware also allows the creation and use of business data that could not previously be meaningfully manipulated. As groupware automates an individual’s work and makes it less time consuming, it allows the individual time to reengineer his/her work to accomplish more in less time.

E-mail[14] is one of many components of groupware. It is also the underlying transport mechanism or messaging layer of the groupware application suite in many groupware products. Any organization using e-mail could be said to be using groupware, but it is true only in a limited sense because there are many other components in addition to e-mail that comprise the groupware application suite.

Figure 9-5 is a graphical representation of the overlap between groupware, the World Wide Web[15], and News Groups (Usenet)[16]

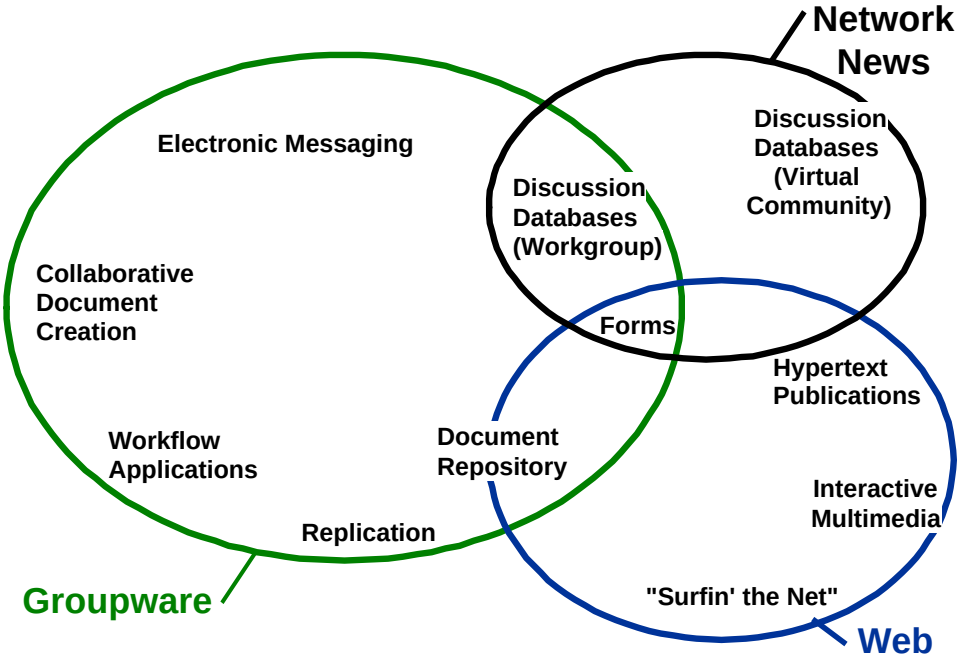


Figure 9-5. Overlap Between Groupware, The World Wide Web, and Usenet

Best Practices

Select applications and infrastructure components from vendors who are committed to complying with and promoting formal standards to implement workgroup computing

Build a groupware strategy based on an electronic mail message handling system-enabled environment that is consistent with DON strategic networking and communication architectures. This strategy allows the scope of work groups to increase over the DON enterprise and facilitates interoperability over disparate communications networks.

Choose groupware products based on their ability to support open systems standards and the client/server model of computing.

14 See Section 6.5 for a complete description of e-mail standards and guidance.
15 See Section 6.7 for a complete description of web standards and guidance.
16 See section 6.8 for a complete description of network news standards and guidance.

9.3.1 Electronic Forms

The majority of today's business forms are still produced on paper. Electronic forms tools, however, reduce a business' reliance on paper and offer capabilities for routing and tracking forms as well as directly inserting information into data bases for optimal service.

Design tools for electronic forms typically allow users or developers to specify the lines, boxes, artwork, and other elements that make form data easier to enter and read. The specification of the data portion of the form includes the information that the user types into the fields. The specification of the form processing component can provide calculation, validation, range checking, database lookup and storage, and forms routing rules.

Client applications for electronic forms allow users to complete forms and participate in a forms routing workflow process. The client applications present the forms to users, accept the input, verify that all required data is entered, and communicate with a server component to process the forms.

Best Practices

Choose an electronic forms product based on its capability to support open systems standards and the client/server model of computing. Be sure to follow the Human Computer Interface (HCI) specifications (Section 7.3.3) when the form also acts as an application interface.

Recommended Implementation

Not determined at this time.

9.3.2 Workflow Management

Workflow management applications typically route documents via an electronic mail message handling system to designated people or applications. Workflow management applications are designed to handle a document through the various stages of processing, presentation, and routing. Typical uses include processes such as purchase orders and document routing. These applications are often viewed as an excellent use of technology for making business processes more productive. Workflow tools can provide significant productivity gains when used in appropriate situations. Often existing mail systems, groupware tools or electronic forms packages can provide the necessary functionality.

Best Practices

Choose a workflow management product based on its capability to support open systems standards and the Client /Server model of computing.

Recommended Implementation

Not determined at this time.

9.3.3 Conferencing

9.3.3.1 Video Teleconferencing

Video conferencing enables people at different sites to simulate face-to-face meetings in real time. Current video conferencing equipment options range from stationary systems installed in dedicated video conferencing rooms to desktop video units. Section 9.4.9 deals with video teleconferencing in depth.

9.3.3.2 Audiographics Conferencing

Audiographics conferencing provides a more cost effective method of conferencing when seeing the conference participants is not required. The audio portion is typically a telephone conference call. The graphics portion is provided over the network and displays an image that can be modified by all participants. The graphics portion provides the enhanced capability beyond a telephone conference call. The graphic is usually referred to as a “whiteboard.”

Audiographic conferencing can be more efficient than video teleconferencing because it frees participants from “visual courtesy.” Participants can perform other work in-parallel when the current conference discussion is not relevant. Discipline must be maintained, however, to ensure that all participants remain sufficiently engaged.

Use audiographics conferencing when viewing and modifying a common graphic or page of a document to enhance a telephone or teleaudio conference call.

Best Practices

Not determined at this time.

Recommended Implementation

Not determined at this time.

9.3.3.3 Text Based Conferencing

Textual-based conferencing requires the lowest network bandwidth of the three types of conferencing. It provides a mechanism that allows conference participants to view each other participant’s input. One of the features of the textual conference is that the text can be saved and referred to at a later time.

Use text-based conferencing as an alternative to telephone conference calls.

Best Practices

Not determined at this time.

Recommended Implementation

Not determined at this time.

9.3.4 Calendaring and Scheduling Systems

The primary benefits of calendaring and scheduling systems include reducing the time needed to schedule meetings and identifying and reserving required resources, including people, conference rooms, and equipment such as overhead projectors.

Calendaring and scheduling can provide the ability to search for the next available time when all required resources are available and define critical and non-critical resources. The systems also allow RSVPs to be accepted or rejected, changes to be made to meeting times and places, or cancellation of meetings. In addition, the systems also provide logs for meetings and personal activities.

Use an enterprise calendaring and scheduling package that supports consistent office procedures and reduces administrative effort.

Best Practices

Not determined at this time.

Recommended Implementation

Select calendaring and scheduling products that conform to TOG XCS API

9.3.5 Group Decision Support Systems

Group decision support systems are designed to increase the effectiveness of meetings. Electronic meeting support systems are decision support systems that can assist in capturing the output of brainstorming sessions, allow voting and ranking of ideas, establish priorities when resources are limited, and store the content and results of group decisions. When using an electronic meeting support system, an impartial facilitator is generally used to keep the meeting moving and to help resolve any disputes among participants. A technographer is generally used to run the master console of the software that is being used to support the meeting.

Best Practices

Use commercial off-the-shelf group decision support products that use DON's standard hardware, software, and network components. Choose group decision support system products based on their capability to support open systems standards and on the client/server model of computing.

Recommended Implementation

Not determined at this time.

9.4 Computer Telephony

Computer Telephony adds computer intelligence to making, receiving, and managing of telephone calls. Computer Telephony can be broken into three broad categories:

Messaging – voice, fax, e-mail, and unified messaging

Transaction processing – Interactive Voice Response (IVR), customer access to enterprise data, and processing of call requests without human intervention

Intelligent phone calls – Inbound and outbound call handling, "Predictive" and "Preview" dialing, information-based call routing, dialog box with customer information, and virtual (geographically distributed) call centers

Messaging and transaction processing are generally available and easy to obtain. These technologies cover predefined markets and are not covered here.

9.4.1 Computer Telephony Integration (CTI)

CTI adds intelligence to phone calls by combining two of the most commonly used business tools – the computer and the telephone. The integration of computers, networks, and Private Branch Exchange (PBX) switches adds intelligence to incoming calls by routing the call to the best person and delivers information about the caller to the person receiving the call. Additional intelligence is added to outgoing calls by placing the call without any human intervention and providing automatic call back, initiation of workflow, guaranteed quality of service for customers, and sophisticated tracking of work.

Currently, the most successful applications have automated existing manual processes. These applications have sound, easily justifiable business cases and can show rapid, measurable return on investment.

CTI solutions generally fall into one of four architectural approaches:

Phone centric – These systems implement a direct connection between switch-connected phones and PCs. This connection with the CTI application allows direct user call control.

Server centric – These systems connect PBX switches to a LAN through an intermediate telephony server, eliminating the physical connection between the PC and the phone. The LAN server routes the data associated with the call, and the PBX routes the call. The information and the call arrive at the workstation in a coordinated fashion. Call centers often use both of these systems to implement comprehensive business solutions.

PC centric – These systems connect both the PBX and the phone to an adapter in the PC. With this approach, the multimedia PC emulates the physical hand set. This approach allows the PC application to manage call control and any incoming media, whether voice or data.

LAN centric – These systems utilize a server on the network, performing the tasks of a PBX and routing calls over the network to a workstation. There is only the network connection to the workstation and no phone line connection.

Implementation of CTI solutions is dependent on sets of APIs that allow desktop computers to control telephone switch equipment. Since the predominant standards are the result of supplier activity, they are de facto in nature.

Best Practices

Select tools that support current de facto standards and enable interoperability.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary Implementations	TAPI V2 TSAPI Tmap S.X00 CSTA VTOA	TAPI V2 TSAPI Tmap S.X00 CSTA VTOA	TAPI V2 TSAPI Tmap S.X00 CSTA VTOA	TAPI V2 TSAPI Tmap S.X00 CSTA VTOA	JTAPI 1.1
Activities, Platforms, Operational Environments		System implementers			

Table 9-4 Computer telephony integration

- TAPI is the Microsoft/Intel Telephony API.
- TSAPI is the AT&T/Novell Telephony Services API.
- Tmap is being developed by Nortel (formerly Northern Telecom) and is designed to enable TAPI-based applications to work with PBX. Tmap itself is not an API set. Tmap provides a link between TAPI and TSAPI, thus giving TAPI the full third-party call control capability that it currently lacks over TSAPI-enabled PBXs. The Enterprise Computer Telephony Forum (ECTF) adopted Tmap, and Nortel committed to developing Tmap according to ECTF specifications.
- S.X00 is the official set of standard APIs (S.100-900) published by ECTF to provide for interoperability.
- Computer Supported Telecommunications Applications (CSTA), an API set defined by the European Computer Manufacturers Association, is supported mainly by European-based PBX suppliers.
- Java TAPI (JTAPI) is the Sun Java interface following TAPI standards.

9.5 Video Teleconferencing

Video Applications run on video teleconferencing systems and networks. These applications also make use of conferencing services available from government and industry. A discussion of entire systems and networks are provided to provide a complete understanding on how the applications are utilized.

Video conferencing for Naval forces ashore and afloat allows geographically dispersed activities to conduct face-to-face meetings in real time. Current video conferencing systems range from reservation based dedicated room systems to portable cart and desktop systems. Emerging are ATM based desktop video systems.

9.5.1 Afloat Video Teleconference Systems

Afloat Naval forces are served by the Video Information Exchange System (VIXS). The VIXS Network consists of ITU-T H.320 capable carts aboard ship connected via DSCS (military) or commercial C band SHF terminals (Challenge Athena) to any one of a number of ITU-T H.243

capable Multi-point control units (MCU's) ashore. These terminals currently range from PictureTel 4000 to 4500 series and are connected to shipboard Video distribution systems. The VIXS terminals are capable of proprietary compression algorithms and operate best while using the PictureTel SG-3 algorithm whenever possible. While SG-4, is available on some fleet units not all MCUS are capable of handling this algorithm. Consideration has been given to incorporate this (SG4) algorithm into the VIXS Network as the DON moves from the legacy system (manufacture discontinued M8000 product) to it's (MT-570) enhanced replacement model.

Best Practices

All systems must be capable of H.320 standard for standards based interoperability when shipboard systems are linked via gateways to other standards based networks.

Recommended Implementation

Proprietary compression algorithms of SG-3 to SG-4 are authorized when like capable terminals are allocated together.

9.5.2 Shore Video Teleconference Systems

9.5.2.1 Shore VIXS Network

Shore terminals within the VIXS network mirror the afloat units except for those where video monitors and cameras are external to the cart and are integrated into room systems with access and gateways to other VTC networks. Both PAC and LANT VIXS Hubs (Multipoint Control Units) have been provisioned with ISDN dial-up access ports to meet the ever-growing (DON and Allied) demand for VIXS access from ISDN capable standards based VTC systems from external shore networks. Dial-up connections can be initiated from either the subscriber or hub site master station. These secure dial-up connections use ISDN BONDING Mode 1, KIV-7 (KG-84 embedded Type 1 Encryption Device) and range in speed from 112Kbps -384Kbps (ref: IAW with FIPS-178). Would be dial-up subscribers are required to submit their Network Admission request to CNO N61 for approval. Once approved, VIXS subscribers are required to establish a system profile and perform validation testing with SPAWAR Systems Center Charleston Code 70. SPAWAR Systems Center Charleston presently validates and maintains all VIXS system profile information on behalf of CNO N61.

Best Practices

Shore access for VIXS will be controlled through designated H.243 standard Multipoint Control Units located in Hawaii, Hampton Roads, Naples, Bahrain.

Recommended Implementation

VIXS multipoint control units must provide support for standards based H.320 and proprietary algorithms of SG-3 at speeds of 112-384Kbps. Migration to SG-4 algorithm across all MCU's is recommended.

9.5.2.2 Deployable Video Teleconference Systems

Deployable VTC packages which are capable of standards based and proprietary algorithms such as the Crash-Out Package (COP) AN/MSQ-126 with the Picturetel 4500.

Best Practices

Deployable systems must comply/interoperate with shore and tactical systems and networks.

Recommended Implementation

Deployable VTC packages such as the Picturetel 4500 which is a part of the Crash-out package (COP) AN/MSQ -126 which is capable of standards based and proprietary algorithms .

9.5.2.3 Non-Tactical Shore Video Teleconference Systems

The predominance of shore systems for Navy and Marine Corps are either CLI Rembrandt (found in most DCTN schedule “D” facilities) and/or Picturetel. Various other vendors are capable of the H.320 standard, however, proprietary algorithms are preferred when like terminals are connected. For CLI Rembrandt, CTX Plus and for Picturetel SG3 and SG-4. These systems range from full-blown room systems (large VTC studios) to smaller cart systems located in offices and conference rooms.

Emerging into the video community are H.320 based desktop systems connecting individuals and small groups together via ISDN in PRI, Tri- BRI or BRI configurations. These installations also allow for fully integrated (easy to use) T.120 collaborative computing applications (application sharing), white boarding, shared clipboard and rapid file transfers. This method has proven to be an effective low-cost method of spreading VTC capability to a growing base of Naval user groups and represents an integrated voice, video, and data application.

While newer desktop systems are capable of operating in an Internet-based TCP/IP environment, this (TCP/IP) type of system is not currently recommended unless a gateway to ISDN (TCP/IP - H.320 gateway device) is provided to handle long haul connections. Further, LAN-based desktop systems be multi-purpose in that the system remains compatible with H.320 systems via an ISDN gateway and compatible to H.323/H.310 systems via the LAN or ATM-capable network. As ATM networks grow, less traffic will be routed to the ISDN gateways.

Best Practices

Maintain interoperability by implementing H.320 standard VTC systems or H.321, H.323 systems with a H.320 WAN gateway.

Recommended Implementation

Proprietary compression algorithms of CTX-Plus and SG-3/SG-4 are authorized within like capable user groups for both multipoint and point to point conferences for H.320 systems. H.261 and MPEG-2 compression standards are recommended for H.323 and H.310 respectively.

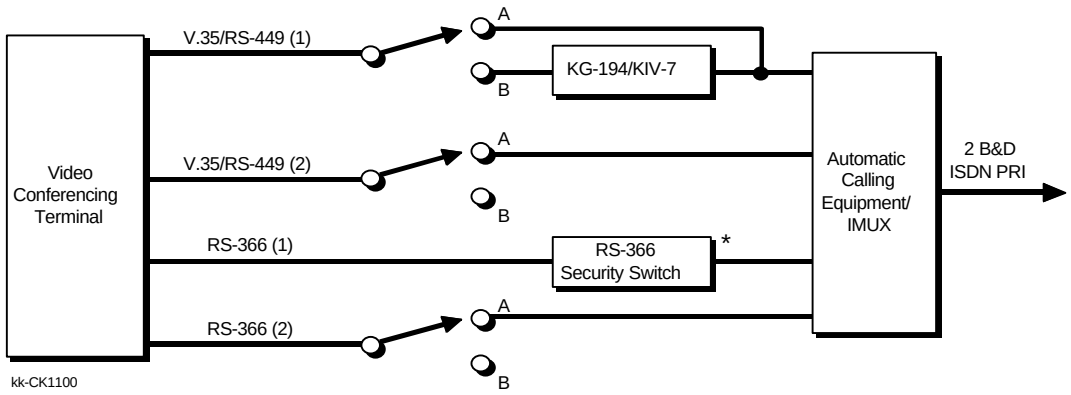
9.5.3 Security

9.5.3.1 Security for Video Conferencing

Security for video conferencing is currently provided by NSA approved type I link encryption equipment. For dedicated transmission paths, CLI Rembrants and VIXS Picturetel carts make use of KG-194's and KG-81's to provide end to end encryption. For dial-up (ISDN) video conferencing, KIV-7's are used due to their low security risk, CIK control, low cost and low profile installation. The VIXS network is a secure only network therefore all connections must be encrypted by either a KG-194 for dedicated connections or by a KIV-7 for dial-up connections. If LAN based TCP/IP video systems are used, the encryption will be moved to the H.323/H.320 ISDN gateway. Emerging equipment slated for possible VTC use are KIV-19's and Secure terminal Equipment (STE release 1 and above).

9.5.3.2 Security for Desktop VTC Systems

Figure 9-6 below suggests a configuration for supporting both classified and unclassified dial-up video conferencing. Additional precautions must be taken to insure TEMPEST integrity through all RS-449 and RS-366 connector. The configuration is notional and it is up to the local Certified TEMPEST Technical Authority (CTTA) to approved such a configuration pending official NSA approval. The suggested configuration is intended to support conferences to the SECRET level and is not intended to support either TOP SECRET or SCI-level conferencing. The system configuration consists of a video conferencing terminal acting as data terminal equipment (DTE) that includes dual V.35/RS-449 data ports and dual RS-366 dialing ports; one encryption device, one RS-366 security switch; and one Automatic Calling Equipment (ACE) such as an Inverse Multiplexor (IMUX). Also shown are three A:B bypass switches.



* Automatic connect and disconnect feature does not require A:B bypass switch

Figure 9-6. Desktop Video Configuration for Supporting Dial-up Classified and Unclassified Conferencing

Best Practices

NSA approved type I encryption devices must be used as follows:

- Dedicated Ship to shore: KG-194
- Dedicated Shore to Shore via DCTN network: KG-194
- Dial-up via VIXS Hub: KIV-7

- Secure Desktop Video via ISDN dial-up: KIV-7
- Secure LAN based Desktop Video via ISDN Wan gateway: KIV-7

9.5.4 Video Networks and Services

As for VTC networks, the Defense Video Service - Global (DVS-G) contract has been awarded to AT&T and has begun to migrate dedicated (current DCTN schedule “D” and “I” customers presently still on the DTC extension contract) rooms over to the DVS-G hubs. The DVS-G seeks to provide fully integrated mix of networks of dedicated connectivity through DISN and Dial-up through Accunet, DISN, FTS-2000, MCI and Sprint connectivity to four (initial) regional hub locations (Figure 9-7).

The DVS-G is not a network as such. It is a video service that provides the following value added features: multipoint conferencing dial-up access, dedicated access, network bridging, classified conferencing (up to TS collateral) variable data rates, reservation/scheduling service (on-line), directory service, help desk and reports (usage and performance).

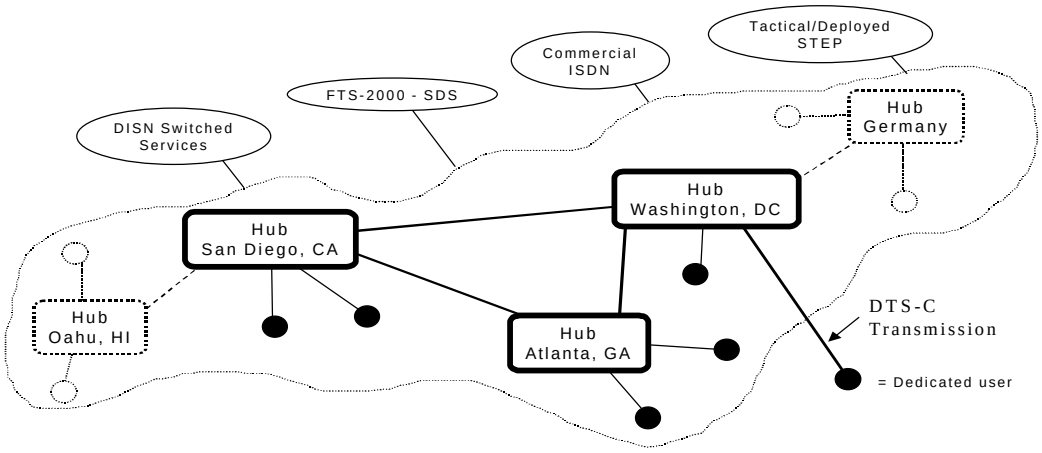


Figure 9-7. DVS-G Video Network Architecture

In addition to boardroom type VTC applications, DVS-G seeks to support a diverse group of DOD video communities such as Tele-training, Tele-medicine and Tele-maintenance. Plans have also been laid to provide video conferencing services for the tactical community (reach-back) through means of Standard Tactical Entry Points (STEP sites) within the Pacific and Atlantic theaters of operation. DVS-G also plans to provide service enhancements to keep in step with emerging Video standards such as ATM.

Other video services may also be used such as local, metropolitan, and regional video hubs due to cost of transmission to national hubs and value added features of support for higher compression algorithms and continuous presence.

Best Practices

Utilize the DISN and commercial networks for dedicated and dial -up connectivity to teleconference via services provided by regional DVS- G Hubs.

Additional regional, metropolitan, or Communities of Interest (COI) hubs are authorized to enhance conferencing services to control costs of connecting to DVS-G provided hubs.

Recommended Implementation

Not determined at this time.

9.5.5 Video Recommended Standards Summary

The ITU-T standards (H.320, H.321, H.323, H.324, and T.120) comprise the core technologies for current and emerging Navy and Marine Corps multimedia conferencing. The T.120 standards address real time data conferencing, the H.320 standards address narrow band videotelephony and terminal equipment over dedicated and switched services such as ISDN. The H.321/H.323 addresses Video communication for LANS and the H.324 standards addresses high quality video and audio compression over POTS modem connections. Table 9-5 provides a framework.

9.5.5.1 H.320 Standard

The H.320 series governs the basic video telephony concepts of audio, video and graphical communications. It specifies requirements for processing audio and video information, providing common formats for compatible audio/video inputs and outputs, and providing protocols that allow a multimedia terminal to utilize the communications links and synchronization of audio and video signals. Like other Multimedia standards, H.320 applies to multipoint and point-to-point sessions. The H.320 suite addresses video conferencing over circuit switch services like ISDN or Switched - 56 and over dedicated media. Companion standards in the H.320 umbrella are H.221- Frame structure for a 64 to 1920Kbps channel in audiovisual teleservices; and H.230- Frame-synchronous Control and Indication Signals for Audiovisual systems.

The H.321 and H.323 are emerging standards barely in use within the DON due to widespread use of systems employing the H.320 standard.

9.5.5.2 H.310 Standard

Standards H.310 and H.321 adapt H.320 to accommodate the increased bandwidth available with ATM and broadband ISDN. For backward compatibility, H.321 retains much of the structure and many of the components from H.320. For example, H.321 includes the H.261 video compression algorithm. H.310 adds the MPEC-2 video compression algorithm that provides high quality video.

9.5.5.3 H.323 Standard

H.323 describes terminals, equipment and services for multimedia communication over Local Area Networks (LAN) which do not provide a guaranteed quality of service such as packet switched networks such as Ethernet or Token ring. H.323 terminals and equipment may carry real-time voice, data and video, or any combination, including video telephony. The LAN over which H.323 terminals communicate, may be a single segment or ring, or it may be multiple segments with complex topologies. It should be noted that operation of H.323 terminals over the multiple LAN segments (including the Internet) may result in poor performance. The possible means by which quality of service might be assured on such types of LANs/internetworks is beyond the scope of this Recommendation. H.323 terminals may be integrated into personal computers or implemented in stand-alone devices such as videotelephones.

Support for voice is mandatory, while data and video are optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media

type can interwork. This recommendation allows more than one channel of each type to be in use. Other recommendations in the H.323-Series include H.225.0 packet and synchronization, H.245 control, H.261 and H.263 video codes, G.711, G.722, G.728, G.729, and G.723 audio codes, and the T.120-Series of multimedia communications protocols.

9.5.5.4 H.324 Standard

This video standard describes terminals for low bit rate multimedia communication, utilizing V.34 modems operating over the GSTN. H.324 terminals may carry real-time voice, data, and video, or any combination, including videotelephony.

H.324 terminals may be integrated into personal computers (and Laptops) or implemented in stand-alone devices such as videotelephones. Support for each media type (voice, data, and video) is optional, but if supported, the ability to use a specified common mode of operation is required, so that all terminals supporting that media type can interwork.

Other Recommendations in the H.324-Series include the H.223 multiplex, H.245 control, H.263 video CODEC, and G.723.1 audio CODEC. The Standard makes use of the logical channel signaling procedures of Recommendation H.245, in which the content of each logical channel is described when the channel is opened. Procedures are provided for expression of receiver and transmitter capabilities, so transmissions are limited to what receivers can decode, and so that receivers may request a particular desired mode from transmitters.

H.324 terminals may be used in multipoint configurations through MCUs, and may interwork with H.320 terminals on the ISDN, as well as with terminals on wireless networks.

9.5.5.5 T.120 Standard

The T.120 standard focuses on collaborative computing, common whiteboard, and applications sharing during any H.32x video conference. The specification also allows data only T.120 sessions when no video communications are required. In addition, T.120 supports multipoint meetings with participants using different transmission media. T.120 defines communication and application protocols and services supporting real time multipoint data communications. T.120 recommendations include:

- T.122 Multipoint Communication Service
- T.123 Network Specific Transport Protocols
- T.124 Generic Conference Control
- T.126 Still Image Exchange

	ISDN H.320	POTS H.324	IP/LANs H.323	ATM H.321	Hi-Res ATM H.310
Guidance	Use where ISDN is the available transport medium . Used in dedicated configurations also	Not recommended	Use where the transport medium is IP over Ethernet, FDDI or ATM. Used in a Non QOS network	Use where the transport medium is ATM cells and the higher performance of MPEG-2 is not required. Used in QOS network	Use where highest performance over ATM cells is required.
Video	H.261	H.261 H.263	H.261 H.263 JPEG	H.261 H.263 JPEG	MPEG-2 H.261 JPEG
Audio	G.711 (NB) G.722 (WB) G.728 (CELP)	G.723	G.711(NB) G.722(WB) G.723(DUAL) G.728(CELP) G.729(CS-ACELP)	G.711(NB) G.722(WB) G.728(CELP)	MPEG-1 MPEG-2 G.7XX
Data	T.120	T.120 T.434 T.84	T.120	T.120 H.281	T.120
Multiplex	H.221	H.223		H.221	H.222.1 H.221
Signaling	H.230 H.242	H.245	H.230 H.245	H.230 H.242	H.245
Multipoint Control	H.243	N/A	N/A	H.243	N/A
Encryption	H.233 H.234	H.233 H.234		H.233 H.234	NIA
External NSA Approved type 1 encryption	KG-194 KIV-7	TBD	KIV-7 at WAN Gateway from Classified LAN	KG-75 Between ATM Nodes; KIV-7 at WAN Gateway	KG-75 Between ATM Nodes; KIV-7 at WAN Gateway

Table 9-5 Video Standards Overview Matrix

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	H.320 (minimum) products for: Room systems, Carts, Desktops, H.243 MCU'S DVS-G Services DISN and Commercial ISDN Networks	H.320 (minimum) products for: Room systems, Carts, Desktops, H.243 MCU'S DVS-G Services DISN and Commercial ISDN Networks H.321/H.323 LAN Video	H.320 (minimum) products for: Room systems, Carts, Desktops, H.243 MCU'S DVS-G Services DISN and Commercial ISDN Networks H.321/H.323 LAN Video	H.320 (minimum) products for: Room systems, Carts, Desktops, H.243 MCU'S DVS-G Services DISN and Commercial ISDN Networks H.321/H.323 LAN Video	IP based only Products (See the note below.)
Activities, Platforms, Operational Environments		All			

Table 9-6 Video Standards

Note

IP-based products is placed in the “Emerging” column because of their sheer commercial popularity. Their use is not recommended at this time because IP-video is not authorized over the DISN.

9.6 Mission Area Applications

Mission area applications implement specific functional user requirements and needs (e.g., payroll, accounting, materiel management, personnel, control of real-time systems, analysis of order of battle). The application software itself may be COTS or GOTS, custom developed, or a combination of these. A number of these mission area applications are being standardized across DOD. In addition to the application software, an information system includes data that can be application specific (e.g., a log of invoices and payments) or an integral part of the software (e.g., application parameters, screen definitions, diagnostic messages). Information systems also include training (e.g., tutorials and on-line help), support tools (e.g., programs for software development, self-test diagnostics), and system management aids (e.g., system administration).

Best Practices

Mission applications shall transition to DII COE and interface to common support applications to the maximum extent possible. Mission applications should consider COTS solutions where possible.

Recommended Implementation

Not provided at this time.

9.7 Application Support Services

Application support services directly support the flow of information throughout the network. These services provide a set of integrated capabilities that the application software entity (Mission Area Applications and Common Support Applications) accesses to obtain standard common operating environment services. The characteristics of the application support services are transparent to the mission and common support applications developer.

9.7.1 General Software Engineering Services

The guidance provided in this general section covers all multipurpose applications, database applications and utility applications. Separate, specific guidance is provided in Section 9.7.2 for web development.

The functionality of an application is embodied in the programming languages and methods used to develop it. Additionally, professional system developers require tools appropriate to the development, maintenance and testing of applications.

Best Practices

According to DoD 5000.2-R, it is DoD policy to design and develop software systems based on software engineering principles and shall apply to all contracted software development.

Utilize the following IEEE standards for software engineering. These standards cover the development, maintenance and testing of software applications.

Specific Policies:

- For General Applications, make use of structured multi-purpose programming languages like C++ and Visual Basic. JAVA may be used as development tools mature sufficiently.
- For Web/Internet Applications, make use of JAVA and CGI. (Active X is not recommended due to lack of security controls and lack of portability across all browsers.)
- For Utility applications (helper applications that provide additional functionality to the operating system), make use of PERL.

Recommended Implementation

See References (Section 9.5) under “Software Engineering.”

9.7.2 Web Development

Java is the latest in a long line of computer programming languages. As the most modern language, it takes advantage of several decades of lessons-learned and incorporates the latest thinking in computer science. Java is probably most easily understood as a better version of the "C" programming language that is easier and safer to use and which was designed from the start with today's object-oriented programming techniques in mind. Java was designed with a goal of "write once, run everywhere." Political and technical challenges have made this goal difficult to achieve, but not impossible. Efforts are also underway to make Java's application performance comparable with any other programming language.

Java can be used to develop either applications that augment a web browser's functionality - called applets - or stand-alone Java applications. The cross-platform nature of Java, combined with support for multimedia capabilities, has also made Java an emerging solution for delivery of multimedia content (presentations packaged as applications).

The Java language is easily extended through the addition of new Java class libraries. Therefore, any standards definition needs to address not just the core language specification, but also the extensions to the language.

The core functionality of Java is contained in the Java Foundation Classes. There are many parallel efforts underway to bring new functionality to Java through the creation of new standardized class libraries. Following are descriptions of many of these initiatives that should be incorporated into the Java language and development tools in the near future.

Java is being extended to tightly couple with the CORBA object framework. Java's distributed computing technology RMI (Remote Method Invocation) is being integrated with the CORBA protocol and the Internet Inter-ORB Protocol (IIOP). JavaSoft is also developing a JavaIDL (Interface Definition Language) specification. Once the IIOP has been extended with some of missing capabilities from RMI, RMI will be phased out. This effort supported by IBM, Oracle, Sybase, Informix, Netscape, and Novell.

Guidelines

Concerns. With any evolving standard there can be confusion among developers as to which version of the standard to work from. During 1997, many developers were still working on version 1.1, even though version 1.1.3 was out and other developers were already working with the beta 1.2 release because it had features they needed not available in previous versions. There is some danger in developing for features that the installed base of Java Virtual Machines do not yet support.

Security. Basic Java security is provided by what is known as the "sandbox model." The sandbox model limits Java applets access to the user's system resources preventing a malicious applet from doing any permanent damage. Java version 1.2 includes an extension of the Java sandbox model to work at the file-system level and the introduction of the scaleable Protection Domain Architecture.

In addition to the built-in "sandbox" protections, Java applets can be controlled through (1) the use of firewalls to keep them out, (2) the use of signed objects to certify that the applet is from a reliable source and has not been tampered with, or (3) the use of proxy applets that keep the executing applet outside the organization’s firewall.

Best Practices

Not determined at this time.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	Java 1.1, 1.2	Java 2.0	Java	Java	J/SQL JBDC Java IDL
Activities, Platforms, Operational Environments		Software Developers			

Table 9-7. Web Development Standards

Notes:

- Oracle, IBM and Tandem have proposed a Java language extension for accessing Relational Database Management Systems (RDBMS) called J/SQL. Every RDBMS supports SQL queries, this extension would allow Java programs to talk to directly to the leading databases. JSQL will be submitted to ISO/IEC for approval as standard.
- In addition to J/SQL there is another database connectivity initiative, known as Java Database Connectivity (JDBC). DBC is a standard set of Java classes that provides vendor-independent access to relational data. JDBC class calls get converted to Open Database Connection (ODBC) and then to vendor specific APIs.
- The International Standards Organization (ISO) has approved Java as an ISO standard. The standard includes the Java Virtual Machine, Java language specification and the Java Foundation Classes APIs. JavaSoft (the Sun Microsystems subsidiary responsible for developing the Java language) was named the organization in charge of maintenance of all the Java specifications. Sun, IBM, and Netscape have set up the Java Porting and Tuning Center to ensure compatibility across all major computing platforms and speed the introduction of Java enhancements.
- Java Development Kit - 1.2 (renamed Java 2 SDK) is now available for download at java.sun.com.

9.8 References

DII COE

Assistant Secretary of Defense Letter, Implementation of Defense Information Infrastructure Environment Compliance of 23 May 1997

Defense Information Systems Agency (DISA); “Defense Information Infrastructure Common Operating Environment (DII COE);” 1 May 1998; http://spider.osfl.disa.mil/dii/ (24 May 1998)

Defense Information Systems Agency (DISA) Standard: CM-400-01-03, “DII COE Integration and Runtime Specification (I&RTS)” 1 July 1997 http://spider.osfl.disa.mil/cm/general.html (24 May 1998)

Defense Information Systems Agency (DISA) DII COE web site: http://spider.osfl.disa.mil/dii/ (24 May 1998)

Defense Information Systems Agency (DISA) web site: http://www.disa.mil/ (24 May 1998)

Software Engineering

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 610.12-1990 IEEE Standard Glossary of Software Engineering Terminology, 1990, http://standards.ieee.org/db/status/ (24 May 1998) (Revision and redesignation of IEEE Std 729-1983)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 730-1989 IEEE Standard for Software Quality Assurance Plans, (Also an ANSI standard.) 1989, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 730.1-1995 IEEE Guide for Software Quality Assurance Planning (Also an ANSI standard.) 1995, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 730.1-1995 IEEE Guide for Software Quality Assurance Planning (Revision and redesignation of IEEE Std 983-1986) (Also an ANSI standard.) 1996, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 828-1990 IEEE Standard for Software Configuration Management Plans (Also an ANSI standard.) 1990, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 829-1983 (R1991) IEEE Standard for Software Test Documentation (Also an ANSI standard.) 1983, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 830-1993 IEEE Recommended Practice for Software Requirements Specifications (Also an ANSI standard.) 1983, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 982.1-1988 IEEE Standard Dictionary of Measures to Produce Reliable Software (Also an ANSI standard.) 1988, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 982.2-1988 IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software (Also an ANSI standard.) 1988, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1002-1987 (R1992) IEEE Standard Taxonomy for Software Engineering Standards (Also an ANSI standard.) 1987, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1008-1987 (R1993) IEEE Standard for Software Unit Testing (Also an ANSI standard.) 1987, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1012-1986 (R1992) IEEE Standard for Software Verification and Validation Plans (Also an ANSI standard.) 1986, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1016-1987 (R1993) IEEE Recommended Practice for Software Design Descriptions (Also an ANSI standard.) 1987, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1016.1-1993 IEEE Guide to Software Design Descriptions (Also an ANSI standard.) 1993, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1028-1988 (R1993) IEEE Standard for Software Reviews and Audits 1993, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1042-1987 (R1993) IEEE Guide to Software Configuration Management (Also an ANSI standard.) 1987, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1044-1993 IEEE Standard Classification for Software Anomalies (Also an ANSI standard.) 1993, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1044.1-1995 IEEE Guide to Classification for Software Anomalies 1995, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1045-1992 IEEE Standard for Software Productivity Metrics (Also an ANSI standard.) [1-55937-258-3] 1992, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1058.1-1987 (R1993) IEEE Standard for Software Project Management Plans (Also an ANSI standard.) 1993, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1059-1993 IEEE Guide for Software Verification and Validation Plans (Also an ANSI standard.) 1993, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1061-1992 IEEE Standard for a Software Quality Metrics Methodology [1-55937-277-X] 1992, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1062-1993 IEEE Recommended Practice for Software Acquisition (Also an ANSI standard.) 1993, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1063-1987 (R1993) IEEE Standard for Software User Documentation (Also an ANSI standard.) 1993, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1074-1995 IEEE Standard for Developing Software Life Cycle Processes 1995, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1074.1-1995 IEEE Guide for Developing Software Life Cycle Processes 1995, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1074.1-1995 IEEE Standard for Developing Software Life Cycle Processes 1995, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1175-1991 IEEE Standard Reference Model for Computing System Tool Interconnections 1991, http://standards.ieee.org/db/status/ (24 May 1998) (Includes STL Language Interconnection Profile Form in ASCII format.)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1209-1992 IEEE Recommended Practice for the Evaluation and Selection of CASE Tools (Also an ANSI standard.) 1992, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1219-1992 IEEE Standard for Software Maintenance (Also an ANSI standard.) [1-55937-279-6] 1992, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1220-1994 IEEE Trial-Use Standard for Application and Management of the Systems Engineering Process 1994, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1228-1994 IEEE Standard for Software Safety Plans (Also an ANSI standard.) 1994, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1233-1996 IEEE Guide for Developing System Requirements Specifications (Also an ANSI standard.) 1996, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1298-1992 (AS 3563.1-1991) Software Quality Management System, Part 1: Requirements [1-55937-289-3] 1992, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1348-1995 IEEE Recommended Practice for the Adoption of Computer-Aided Software Engineering (CASE) Tools (Also an ANSI standard.) 1995, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1420.1-1995 IEEE Standard for Information Technology —Software Reuse—Data Model for Reuse Library Interoperability: Basic Interoperability Data Model (BIDM) 1995, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1420.1a-1996 IEEE Guide for Information Technology — Software Reuse-Data Model for Reuse Library Interoperability: Asset Certification Framework 1996, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1430-1996 IEEE Guide for Information Technology — Software Reuse-Concept of Operations for Interoperating Reuse Libraries (Also an ANSI standard.) 1996, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE J-STD-016-1995 EIA/IEEE Interim Standard for Information Technology Software Life Cycle Processes Software Development Acquirer-Supplier Agreement (Issued for Trial Use) 1995, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1295-1993 IEEE Standard for Information Technology-X Windows System-Modular Toolkit Environment (MTE) (Also an ANSI standard.) 1993, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 662-1992 IEEE Standard Terminology for Semiconductor Memory (Also an ANSI standard.) 1992, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1149.1b-1994 Supplement to IEEE Std 1149.1-1990, IEEE Standard Test Access Port and Boundary-Scan Architecture (Also an ANSI standard.) 1994, http://standards.ieee.org/db/status/ (24 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE 1149.1-1990 IEEE Standard Test Access Port and Boundary-Scan Architecture (Also an ANSI standard.) 1990, http://standards.ieee.org/db/status/ (24 May 1998)

10. Enterprise Management

This chapter includes the enterprise management organization, information system monitoring and controls, integrated network management, and proposed measures of effectiveness for the information infrastructure. The relationship of this chapter with the ITSG is shown in Figure 10-1.

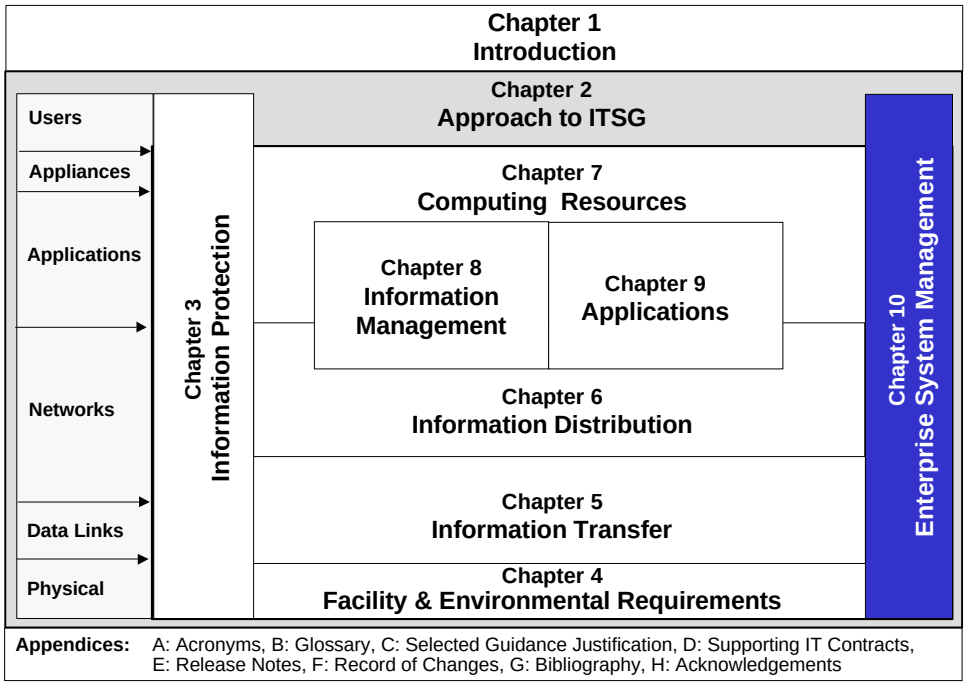


Figure 10-1. ITSG Document Map highlighting Chapter 10, Enterprise Management

10.1 Introduction

Enterprise management encompasses information systems and integrated network management. Enterprise management supports procedures and tools that maintain the integrity and efficiency of IT resources. The procedures and tools support proper planning, configuration, and problem solving. Network and cable management, resource management, systems administration, and security systems all fall within the scope of enterprise management.

The enterprise management framework provides the following:

- Integrated approach to managing diverse networks and information systems
- Environment for developing and integrating management applications
- Structure in which management applications can operate consistently
- Basis for delivering IT services to customers according to predefined levels
- Features provide a flexible and scalable platform for managing change, complexity, and cost-of-ownership

Management of the entire IT spectrum is needed to achieve the seamless, single-system performance of the complete Naval enterprise called for under the DON CIO management strategy. Information systems include those components required to provide voice, audio, video, imagery, and data services to our customers. In presenting the standards guidance, this chapter

includes a proposed integrated management strategy for the entire information infrastructure – including applications and computing resources. Rationale: standards for enterprise management can have little relevance unless there is a DON enterprise strategy for providing these services to an integrated Naval information infrastructure. Enterprise management is a critical part of the infrastructure foundation.

Enterprise management encompasses enterprise-wide organization, systems monitoring, control, and quality. Each of these elements is addressed to orchestrate the implementation of information technologies throughout the DON infrastructure. Enterprise management is similar to information protection in that it spans all technology layers (Figure 10-1). Addressing system control and quality together connects the infrastructure control mechanisms (system control) and the infrastructure feedback (system quality) providing a complete control-response loop.

Figure 10-2 illustrates the context for system control and quality over a representative architecture. System monitoring or control processes must be present in each system component of the architecture from the appliances in each local area network to the network node devices in each wide area network.

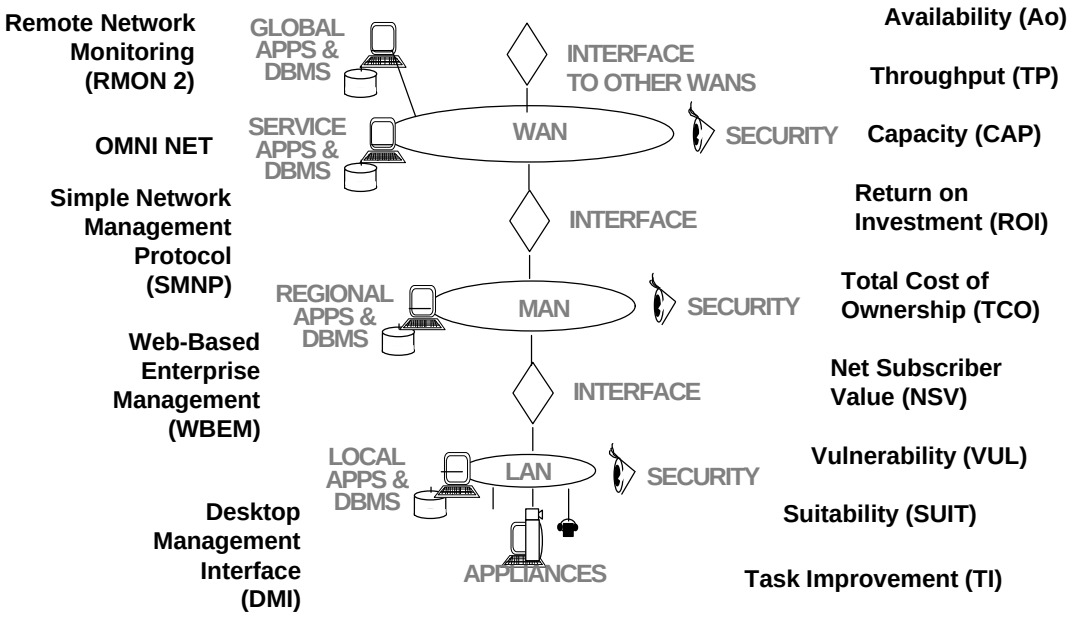


Figure 10-2. Enterprise Management Standards and Guidance in the context of the enterprise system architecture

Enterprise system control and quality measurement is impossible without an organizational structure that permits assignment of responsibility for system monitoring, control, and quality. The organizational structure has assigned enterprise management functions at appropriate commands in order to aggregate system metrics for total system quality. The next section of this chapter outlines an organizational management framework.

- Section 10.1 - Overview
- Section 10.2 - Organizing for Enterprise Management
- Section 10.3 - System Monitoring and Control Standards Guidance
- Section 10.4 - System Quality

10.2 Organizing for Enterprise Management

The enterprise management organization must support the full scope of services and systems. It must address the current system implementation, as well as the evolution of the infrastructure and applications as technologies and command missions change.

Best Practices

The Navy and the Marine Corps will establish an integrated community of Information Technology Service Centers (ITSCs) that support warfighters, operational users, and support personnel by implementing, operating, and managing the DON's comprehensive information infrastructure. This infrastructure includes all systems that transport, process and store information including tactical and non-tactical; classified and unclassified; voice, video and data systems. Systems that comprise the infrastructure will be integrated to the maximum extent practical so that operators view the infrastructure as a single system covered by a single support group.

Recommended Implementation

The following provides the guidance and concept for managing the DON's enterprise information infrastructure.

10.2.1 Enterprise Management

There are multiple dimensions of enterprise management that must be understood to adequately address the full scope of functions performed, objects managed, and level of management focus. To accomplish this we introduce and define three dimensions of enterprise management for the purpose of addressing enterprise management standards.

- Enterprise Management Functions
- Enterprise Component Categories
- Command Echelon/Area of Geographic Coverage

10.2.1.1 Enterprise Management Functions

Table 10-1 outlines the enterprise management functions that must be supported.

System Implementation	System Operations	System Support
Configuration Management	System Control	Personnel
System Architecture	System Configuration	Accounting
Systems Engineering	Storage Management	Asset Management
Systems Integration	Fault Management	Administration
System Analysis	Performance Management	Billing
Cost Analysis	Security Management	
Acquisition	Help Desk	
Installation	Service Desk	
Testing	Logistics Support	
Training		

Table 10-1. Enterprise Management Functions

10.2.1.1.1 System Implementation

System implementation includes functions that prepare and implement changes to the DON enterprise technical infrastructure. It includes management of cable plant, hardware devices, software licenses, network services, circuit provisioning, commercial applications and tactical/business applications. The support organization will provide orderly system changes and implementation.

Industry standards have yet to address the greater role of system implementation and configuration management software, hardware, and network resources. The X.700 (OSI) Software Management function and POSIX 1003.7 provide software administration and distribution guidelines.

10.2.1.1.2 Systems Operations

Systems operations includes eight functions that support and control the currently implemented infrastructure.

10.2.1.1.2.1 System Control

System control involves taking specific action against network and system components to change their status. This includes controlling the configuration and definition of the resources. Control of the network from a workstation, control of the network configuration, controlling remote processors, and controlling operating system resources are all examples of system control. Note that realtime dynamic control of resources in tactical networks, e.g. aboard ship, is best handled locally and is generally not feasible or practical to accomplish from a centralized, infrastructure-wide system control mechanism.

10.2.1.1.2.2 Systems Configuration

The Systems Configuration will address elements such as moves, adds and changes occurring in the user population. No industry standard yet exists.

10.2.1.1.2.3 Storage Management

Storage management provides for the backup and recovery of systems through system and network data collection and logging. Storage management protects critical data stored, including all database and application backups, from unauthorized use, overwriting, or deletion. It automatically archives data before you run out of disk space, and transparently restores the data when you need it.

- Hierarchical storage management features will also be provided. Dynamic placement of data across various storage technologies, such as memory, disks, and tapes, based on usage and retention parameters

10.2.1.1.2.4 Fault Management and Performance Management

Fault management involves fault identification, isolation, recovery, resolution, and message filtering. The system must identify and correct systems faults at control centers before the user detects the problem. Faults identified by users must be acted upon and solved promptly. A tracking system will allow the user to determine the status of problem resolution.

Performance management involves the continuous monitoring of system performance. It requires trend analysis as well as system modeling and simulation to determine when system upgrades are required. Control centers should have remote monitoring and diagnosis capabilities on wide area network equipment that address both the network and end-user equipment.

X.700 (OSI) standards exist for fault management and performance management. Also, TOG's XIMS defines many operational services such as alarm, event, and scheduling management.

10.2.1.1.2.5 Security Management

Security management addresses access to the system including user accounts, certificate administration, firewall management, encryption, system certification and accreditation support. Security management must provide solutions for information-at-rest as well as information-in-transit, and must account for emerging requirements for multiple release categories such as NOFORN, NATO, coalition partners, Partners for Peace, etc. The ITSC organization (discussed in Section 10.2.2.1) will implement intrusion detection systems, perform vulnerability assessments and provide malicious code (virus) detection. The organization will establish a reporting scheme so that detected and user-reported security incidents are promptly acted upon by the security or law enforcement agency.

For information about security, see Chapter 3, Information Protection.

10.2.1.1.2.6 Help Desk and Service Desk Customer Interface

The ITSC Help Desk is the front line interface to the users to resolve issues associated with IT services. The Service desk is the front line outreach center to minimize disruption to user operations during system upgrades and configurations changes. The Service Desk supports change control, coordination, approval, and implementation.

Both the Help Desk and the Service Desk require a standard customer interface. The customer interface function collects requirements from and coordinates with the users of services. User requirements include change requests, requests for additional services, requests for new services,

and problem requests. The consumer interface function tracks requests and problems until resolution and provides feedback to the users. No industry standard exists at this time.

10.2.1.1.2.7 Logistics Support

Applications are available to track inventory of IT consumables and provide notice when it is time to reorder. The IT Logistic Support System should be coupled with the Asset Management System. No standard yet exists.

10.2.1.1.3 System Support

The five functions under the system support category are personnel, accounting, billing, asset management, and administration. Of these, ITSG standards guidance is applicable to accounting, asset management and billing.

10.2.1.1.3.1 Accounting

Accounting maintains costs and expenses associated with the use of IT resources. Advanced accounting capabilities support a breakdown of the use of shared resources. Accounting also encompasses software metering.

Both X.700 (OSI) and TOG's XRM define accounting standards.

10.2.1.1.3.2 Asset Management

Asset management provides a repository of accurate and timely data about managed resources. Inventories are used to track expected occurrences of the resources against the actual existence of the resources. Inventories may also include various reference information such as location, owner, or supplier contact.

No industry standards exist for this function.

10.2.1.1.3.3 Billing

A modern billing capability must be provided for those shore/base enterprise environments that use the MAN/WAN facilities of telecommunication service providers. The fundamental function of a billing system is to provide Navy and Marine Corps service centers with an invoice for telecommunication provider network usage and support Naval business and cost of operation objectives. This capability need not be provided for Navy and Marine Corps owned and operated networks in the shipboard environment.

No industry standards exist for this function.

10.2.1.2 System Component Categories

The following outlines the system component categories that must be managed.

> **Appliances**. The hardware, software, and associated peripherals that the operator use to interface with the system. This includes computer clients, servers, printers, telephones, video teleconferencing (VTC) equipment, and associated software.

Communication Circuits and Equipment. The underlying communication circuits, cryptographic equipment, and termination equipment associated with the network. This includes terrestrial communications circuits, wireless (cellular) area coverage, line-of-sight radio, and Satellite Communication (SATCOM) as well as the associated radios, crypto, modems, CSU/DSU, and CODECs. This category focuses on layer 1 (physical) and layer 2 (data link) of the OSI model.

Network. The nodes and circuits that establish fault tolerant, interconnected paths between command elements. This includes the selection and configuration of routers, switches, gateways, bridges and associated addressing schemes and domains. This category focuses on layer 3 (network) and 4 (transport) of the OSI Model.

Basic Network and Information Distribution Services (BNIDS). The core services needed to provide basic information dissemination. This includes the selection and configuration of domain name services, directory services, web services, network news service, electronic mail, and file transfer methods. This and the remaining categories focus on the basic elements of layers 5 and up (session, presentation, and application) of the OSI Model.

Voice. Telephone equipment and services.

Video. Video teleconferencing (VTC) and television equipment.

Servers. Computers, including workstations and mainframes, that provide information services to a network.

Commercial Applications. Commercial software applications.

Operational Applications. Government developed tactical/non-tactical applications such as the Global Command and Control System (GCCS) or Global Combat Support System (GCSS).

10.2.1.3 Command Echelon / Geographic Area of Coverage

The command echelon and geographic area of coverage that must be supported are defined in the following:

Global. The collection of organizations that have enterprise-wide responsibilities. They include the Secretary of the Navy (SECNAV) Staff, the Chief of Naval Operations (CNO), the Commandant of the Marine Corps, the System Commands and Naval Bureaus.

Fleet/Theater. Organizations responsible for the underway fleet, deployed Marines, and theater forces. These include the Fleet Commander-in-Chief (CINC) associated force commanders and type commanders. (“Fleet” is used in lieu of “Fleet/Theater” for brevity throughout this chapter.)

Regional. Organizations responsible for the operations of primarily shore-based or in-garrison commands located within a wide geographic area.

Base, Post, Camp, Station. Organizations responsible for supporting commands within a local area or campus.

Unit. A command with an operational or support mission.

Element. Aircraft, other vehicles, or members of a unit that detach and conduct missions, operations, or support.

10.2.2 Concept of Operations

In the model below (Figure 10-3), rows represent system component categories and columns represent corresponding management functions that support each category. This support has to cover each command echelon from the global down to the command element.

Scale: Naval Fleet Regional Unit Element	OPERATIONS								IMPLEMENTATION										SUPPORT			
	Sys Control	Storage Mgt	Fault Mgt	Perf. Mgt.	Security Mgt.	Help Desk	Service	Logistics	Config Mgt	Sys. Engr	Syst. Arch.	Cost Anal.	Syst. Anal.	Syst. Intgr.	Acquisition	Implement.	Testing	Training	Accounting	Asset Mgt.	Admin	Personnel
Oper Apps																						
Coml Apps																						
Data Base Mgt																						
Video																						
Voice																						
Net Services																						
Network																						
Transmission																						
Appliances																						

Figure 10-3. Matrix of Enterprise Management Functions, System Component Categories and Geographic Coverage

The following items and succeeding paragraphs describe support for the enterprise management elements depicted in Figure 10-3.

- Information Technology Service Centers (ITSC)
- Integrated System Management Tools
- System Control and Maintenance
- Application and Information Service
- System Implementation Support

10.2.2.1 Information Technology Service Center (ITSC) Concept

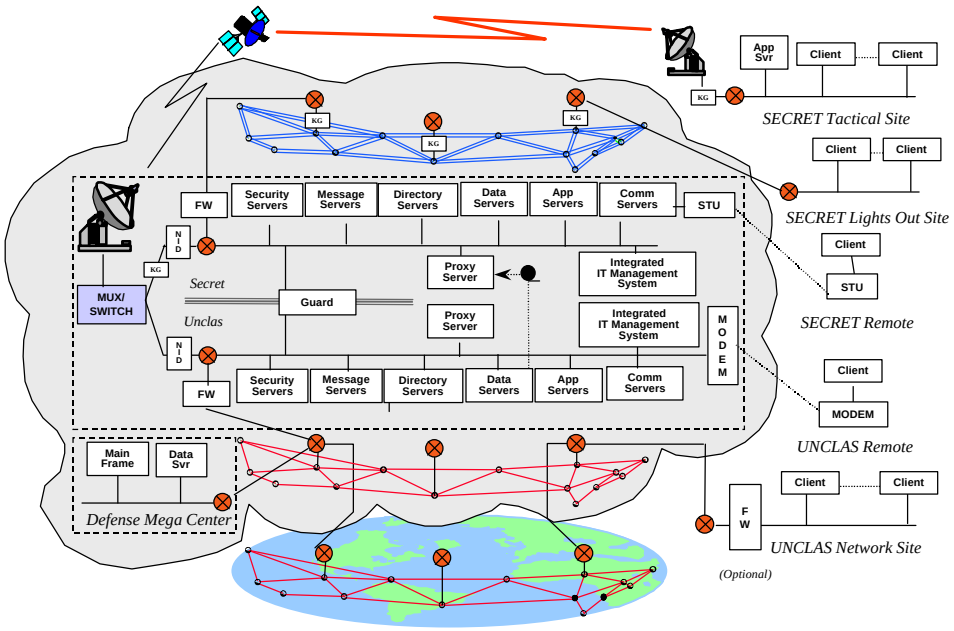


Figure 10-4. ITSC Functions Including Enterprise Management, Interface and Centralized Computing Services

An Information Technology Service Center (ITSC) would provide comprehensive IM/IT support to the DON IT infrastructure. This includes information system operation, implementation support, and administration for a community of information producers and consumers. The ITSCs would be "Local Control Centers" in full compliance with the Joint Defense Information Infrastructure (DII) Control Centers (CC) Concept of Operations (CONOPS). Figure 10-4 illustrates.

Each ITSC would perform three major duties:

- Integrated information system implementation, control and maintenance.
- Interface information flow from network to network including dial-in service.
- Consolidated information/application repository and distribution center for individual commands in the region.

10.2.2.1.1 ITSC Framework and Scope of Coverage

To provide a framework for consolidation on a global scale, as well as services close to the user, enterprise coverage is described with varying scope of coverage. The ITSC goal would be to achieve efficiency through consolidation, but not at the expense of reliability and quality service.

Global Information Technology Services – Service to the entire enterprise. For fault tolerance, at least two sites need to provide global ITSC service.

Fleet/Theater Information Technology Services – Services to the fleet units that are primarily underway or deployed. These ITSCs will be aligned with the Fleet CINCs.

Regional Information Technology Services – Services that support all Naval commands within a geographic region. The majority of information service functions are included in the scope of this service.

Joint Information Technology Services – Services that support non-Naval commands within a concentration area primarily operated by the U.S. Navy or Marine Corps. Hawaii and Norfolk are examples of concentration areas for Naval-sponsored joint commands – USPACOM and USACOM.

Base Information Technology Services – These services would be an extension of the Regional Information Services where physical presence is required. Services in this echelon would be primarily hardware-related such as device and cable plant maintenance, component replacement, software distribution and dial-in service. Since these services need to be performed at remote locations, they would be designated as *Information Technology Outreach Centers* (ITOCs) and serve as the base "store front" for the ITSC.

10.2.2.2 Integrated Enterprise Management Tools

The Joint DII Control Centers CONOPS provides a description of the Joint DII Control System, which includes system element management systems, general system support tools, deployed system support tools and information assurance tools. Shown in Figure 10-5 is the Joint DII CONOPS model applied to the ITSC concept. On the left side in the vertical stack of boxes are the control and monitoring tools. These tools are associated with the technologies listed to their left and roughly align to the seven layer ISO model. Across the top are the security control and management tools. Across the bottom are the overarching enterprise management tools. All of the tools are focused by the Integrated Information Technology Management System (in the center of the diagram) that the ITSC system managers use to monitor and control.

All ITSCs will have access to all enterprise management tools in the Integrated Information Technology Management System, although the tools themselves will not be physically located at every ITSC. Economy-of-scale is achieved by a single global management system, however, quality service is normally best achieved when it is delivered directly to the customer. To optimize economy and quality, system elements that can be managed remotely will be managed centrally (e.g., trouble ticketing). Enterprise management elements that require physical presence will be performed locally. For example, ITSCs and ITOCs that require physical presence to troubleshoot and maintain systems would have the necessary management tools on location. As a general rule, software and network management tools would tend to be centralized at the global ITSC and hardware monitoring and diagnosis tools would be distributed to the localities(ITOCs).

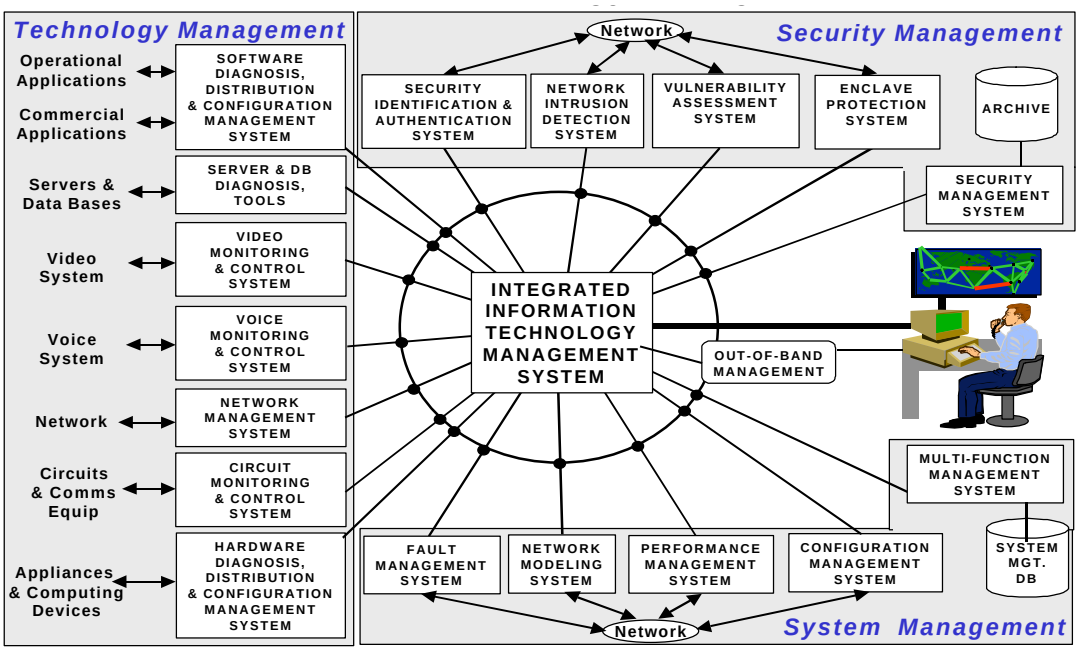


Figure 10-5. ITSC Information Technology Management Tools

10.2.2.3 System Control and Maintenance

ITSC staff personnel would use the Integrated Information Technology Management System to analyze the system performance for tuning and planning, and to monitor and respond to system faults. Trouble tickets will be provided to the appropriate system support activities that dispatch the resources to resolve problems.

10.2.2.4 System Implementation Support

A goal of the DON CIO is to achieve system integration by shifting from application-based enterprise management to infrastructure-based enterprise management. Instead of having a LAN, workstation and server for each application, the infrastructure is developed, supported and evolved as a single system. Traditional tactical/functional programs would transition from developing their own independent infrastructure to developing operational or business applications that utilize the infrastructure. Infrastructure components will be implemented in the same manner. Under the ITSC concept, a coordinated enterprise effort would support existing installations. System Commands and Naval Bureaus would continue to develop and acquire applications to install onto the infrastructure. In its fully realized form, the DON CIO would coordinate with the development and acquisition communities to stand up Integrated Product Teams (IPTs) that are responsible for developing, testing, installing, setting up training and logistic support of specific functional systems.

10.3 System Monitoring and Control Standards Guidance

Section 10.2.1.1 described the management functions as one dimension of total enterprise management. Monitoring and control specifications are needed to build tools and procedures to support these functions. Enterprise management specifications are just beginning to provide monitoring and control capability that support enterprise services.

Enterprise management specifications support both manager/agent and object-oriented management structures.

- The manager/agent structure represents a traditional approach with agents throughout the infrastructure that interact across consolidated, hierarchical monitor and control facilities, called managers.
- The object-oriented structure is an approach in which all resources, services, and management applications appear as objects and interact as peers. Using object orientation, differences among various technical elements may be abstracted so that information and control appear to be the same. For example, a common command is issued to query the status of a device. If that query is sent to an object representing the device, the object could internally perform the device-dependent query and translate the result into a commonly understood status.

Several standards continue to evolve. In the data networking area, Simple Network Management Protocol (SNMP), and Remote Network Monitoring 2 (RMON 2) standards are established and continue to proliferate in the United States in emerging products. Although version 2 of SNMP has been available for several years and addresses important issues of expanded security and performance, low industry acceptance has resulted because competing security approaches could not be resolved. Recent drafts of SNMP Version 3 (SNMP 3) contain security features that are expected to receive wide industry acceptance..

The RMON 2 specification is gaining popularity because it provides centralized enterprise management for complex networks with less network coordination than SNMP. The Desktop Management Task Force (DMTF) consortium is defining desktop APIs for monitoring and controlling personal workstation hardware and software resources. The resultant product is called the *Desktop Management Interface* (DMI). In the telecommunications area, the telecommunications management network (TMN) is the management architecture standard specified by CCITT/ITU-T. TMN is a basis for the internetworking of various network components and management systems for mainly public telecommunications networks.

The following provides guidance on enterprise management implementation of standards and specifications.

Best Practices

Use management systems and protocols that minimize non-payload overhead and that can be assembled into an integrated system to control and monitor all aspects of the entire infrastructure from a single workstation.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	SMNPv1 RMON 2 XSM	SMNPv1 RMON 2 XSM	SMNPv3 RMON 2 XSM	SMNPv3 RMON 2 XSM	DMI WBEM DMTF V2.0
Activities, Platforms, Operational Environments		ITSCs and Shore. Bandwidth consumption must be considered prior to use for Ships, Ground, and Aircraft			

Table 10-2. System Monitoring and Control Recommended Implementation

10.3.1 The X.700 Series and XSM

Of the few supporting standards supporting enterprise management functions, the most complete are the ITU-T X.700 series. While the X.700 is accepted by the ITU-T, the ISO and the IEC, commercial support of the X.700 is very limited. A declaration that X.700 series is the enterprise management standard would provide little support for advancing the DON towards system integration. The completeness of the X.700 series, however, makes it attractive as a potential standard. Figure 10-6 provides an overview of the X.700 series of enterprise management specifications. The most commonly used specification of the X.700 series is X.711, the Common Management Information Protocol (CMIP), which is comparable to the Simple Network Management Protocol (SNMP).

The X/Open System Management (XSM) by The Open Group (TOG) specification profile effort captures the X.700 series standards.XSM is a comprehensive framework for managing networks and systems from the perspective of the services they deliver to end customers. The goal is to facilitate the automation of information system service management while addressing legacy management system integration and transition to distributed management systems. XSM promotes management software that allows an administrator to manage heterogeneous systems networks as a single logical system.

OSI System Management Architecture

Title	ISO/IEC Designation	ITU-T Designation
OSI Management Architecture		
Management Framework for OSI	7498-4	X.700
Systems Management Overview (SMO)	10040	X.701
OSI Management Communications		
Common Management Information Service Definition (CMIS)	9595	X.710
Common Management Information Protocol (CMIP)	9596-1	X.711
CMIP PICS Proforma	9596-2	X.712
Basic Management Communications	AOM-11	
Enhanced Management Communications	AOM-12	
OSI Management Information		
Management Information Model	10165-1	X.720
Definition of Management Information (DMI)	10165-2	X.721
Guidelines for Definition of Managed Objects (GDMO)	10165-4	X.722
Requirements and Guidelines for Implementation Conformance Statement Proformas associated with OSI Management (MOCS Guidelines)	10165-6	X.724
OSI Generic Definitions – Systems Management Functions		
Object Management Function	10164-1	X.730
State Management Function	10164-2	X.731
Attributes for Representing Relationships	10164-3	X.732
Alarm Management Function	10164-4	X.733
Event Report Management Function	10164-5	X.734
Log Control Function	10164-6	X.735
Security Alarm Reporting	10164-7	X.736
General Management Capability	AOM211	
Alarm Reporting and State Management Capabilities	AOM212	
Alarm Reporting Capabilities	AOM213	
General Event Report Management	AOM214	
General Log Control	AOM231	
Security Audit Trail Function	10164-8	X.740
Objects and Attributes for Access Control	10164-9	X.741
Usage Metering Function	10164-10	X.742
Metric Objects and Attributes	10164-11	X.739
Test Management	10164-12	X.745
Summarization Function	10164-13	X.738

Title	ISO/IEC Designation	ITU-T Designation
Confidence and Diagnostic Test Categories	10164-14	X.737
Scheduling	10164-15	X.746
Management Knowledge Function	10164-16	X.750
Change-Over Function	10164-17	X.751
Software Management	10164-18	X.744
Domain Policy Management	10164-19	X.749
Time Management	10164-20	X.743
Generic Network Information Model		M.3100
Alarm Surveillance		Q.821
Performance Management		Q.822
Security Function Profiles	AOM24	
Metric Objects and Attribute Profiles	AOM22	
Summarization Function Profiles	AOM253	

Key:

OSI – Open System Interconnect

ISO – International Standardization Organization

IEC – International Electrotechnical Commission

ITU-T – International Telecommunications Union – Telecommunication Standardization Sector

Figure 10-6. X.700 Series Specifications and Related ITU Proposals

10.3.2 Industry Specifications

Today's networks are predominantly hybrids. Government and industry organizations are meshing managed services from public telecommunications providers with their own private enterprise networks to provide high quality service with fewer operational problems. No single management technology or specifications can deal with the complexity of the hybrid networks. Effective end-to-end management is achieved by selecting a combination of technologies that provides complete function coverage, wide commercial usage, and promise of technology support.

The appropriate management scheme is a combination of industry-proposed and vendor-specific specifications. SNMP and CMIP are the dominant network management protocols. SNMP and RMON2 are the primary specifications for network communications management, Desktop Management Interface (DMI) is appropriate for computing resource management, and Web-Based Enterprise Management (WBEM) is appropriate for internet-based network middleware services. CMIP is the network management protocol most widely promoted by the telecommunications industry. ITU-T Telecommunication Management Network (TMN) is the primary specification for the public data and voice telecommunications networks. Figure 10-7 shows these specifications as applied to the ITSC Information Technology Management Tools.

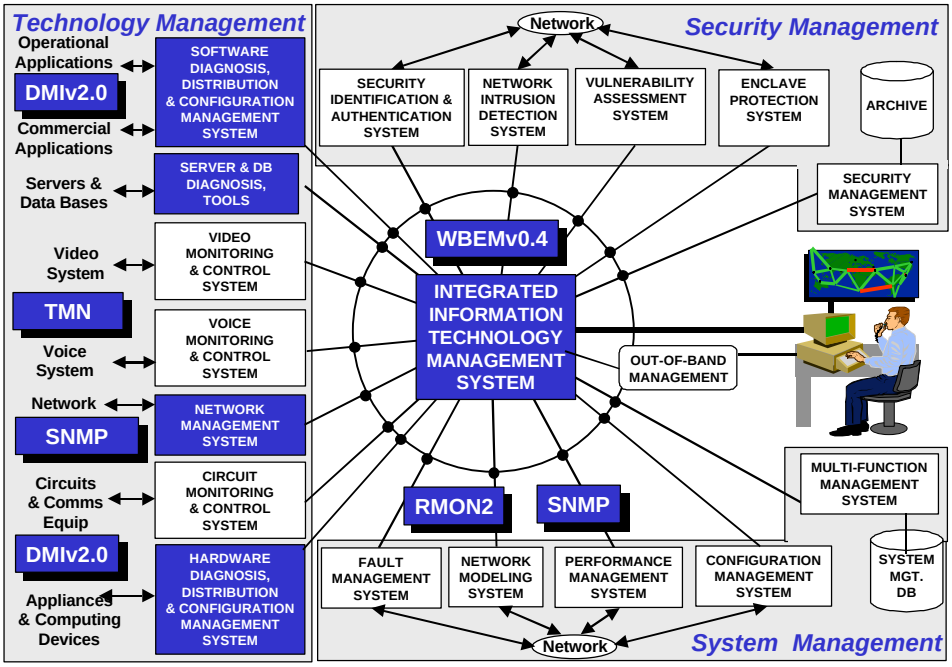


Figure 10-7. SNMP, RMON 2, WBEM and DMI relationship to the ITSC Information Technology Management Tools

10.3.2.1 Simple Network Management Protocol (SNMP).

SNMP version 1 (SNMPv1) is the JTA mandated standard for network management. The greatest advantage to SNMP is that its design is simple and expandable, and easy to implement on a large network. Originally intended as an interim network manager, wide usage of SNMP ensued before more advanced network management protocols such as CMIP appeared. Security concerns have been addressed in version 2 of SNMP (SNMPv2); however, SNMPv2, like CMIP, is neither simple nor in wide use. Although the JTA mandates SNMPv1, use of RMON 2, CMIP or SNMPv2 to avoid the security vulnerability of SNMPv1 is encouraged to build operational experience and offer a migration path from SNMPv1.

The output from the SNMPv2 Working Group did not become a widely accepted standard primarily because two competing security approaches could not be resolved. The SNMPv2 standard provides major improvements over SNMPv1 in two major areas that are important to the management of large enterprises. SNMPv2, through the GetBulk command, increases the amount of management data that can be transferred in a single transaction, thus reducing the potential for heavy data loads and provides a decentralized network management scheme that is useful in large networks where a centralized approach would be cumbersome at best.

Recently a draft standard for SNMPv3 was completed which includes the functionality of SNMPv2 and incorporates the security features found in the proposed security approaches. SNMPv3 includes 3 modules:

- The Message Processing and Control module handles SNMP message creation and parsing functions, and also determines if proxy handling is required for any SNMP message.
- The Local Processing module performs access control for variable binding data, processing that data and trap processing.

- The Security module provides authentication, and encryption functions, and checks the timeliness of certain SNMP messages.

Expectations are that SNMPv3 will succeed in the marketplace and products meeting this standard will now start to appear.

10.3.2.2 Remote Network Monitoring Version 2 (RMON2)

The RMON 2 specification supports monitoring of the network and network devices from selected nodes on the network. The distributed network monitoring and control capability allows more control over large, complex networks with less management overhead. System statistics can be accumulated by remote devices and uploaded to the primary management system upon demand. RMON2 provides an end-to-end view of the traffic flow across the global, enterprise network. It provides network statistics, packet filter, and capture for complete distributed protocol analysis, and provides statistics at the application layers of the protocol stacks. This capability gives the system manager better visibility of network assets.

10.3.2.3 Web-Based Enterprise Management (WBEM)

WBEM is the most promising specification for the Integrated Information Technology Management System (Figure 10-5 and Figure 10-7). Its web-based hypermedia interface is very attractive because of its comprehensiveness and flexibility. WBEM promises to support SNMP, DMI, and ultimately CMIP, as well as vendor-specific specifications. In addition to standard web specifications for HyperText Transfer Protocol (HTTP) and HyperText Markup Language (HTML), WBEM uses:

- HyperMedia Management Schema (HMMS) as an extensible data model representing the managed system environment.
- HyperMedia Managed Object (HMMO) as a managed entity that has data that can be either interrogated or managed by a browser either directly or through a management schema. Every framework object must have at least one URL.
- HyperMedia Object Manager (HMOM) as a management application that aggregates management data and uses one or more protocols to present a uniform representation to the browser using HTML. The HMOM could be implemented using existing development platforms such as Java, Active X, CGI, CORBA or COM. It provides a hierarchical control point for accessing and managing other HMMOSs on the network, services to manage large numbers of managed objects, gateway agents to map HTTP requests for the native protocol of the non-HMMO entities such as SNMP and DMI.

WBEM is considered to be an emerging standard with recommended compliance required for shore and ITSC operational environments. Bandwidth requirements must be assessed before WBEM is recommended for ship, ground, space, or air operational environments.

10.3.2.4 Desktop Management Interface (DMI)

DMI provides an interface between all computing resources (hardware, software, and peripherals) and the management system. It is designed to be independent of any specific computer, operating system or management protocol. It can be used locally, or remotely via a network using remote procedure calls. It is mappable to existing network management protocols including both SNMP and CMIP. DMI was developed by the Desktop Management Task Force (DMTF) and consists of the following elements.

- A format for describing management information
- A service provider access point
- Two sets of APIs to the service providers, one for the management application and a second for the components
- A set of services to facilitate remote management

10.3.2.5 Telecommunications Management Network (TMN)

Telecommunications carriers today must rapidly introduce and manage new competitive service offerings. This means quick integration of state-of-the-art communications equipment from multiple vendors. In response to the challenge of successfully integrating huge numbers of new network elements into the existing network, the carriers and international standards bodies have defined a solution called the “Telecommunications Management Network” or “TMN.” TMN consists of a series of interrelated national and international standards and agreements which provide for the surveillance and control of telecommunications service provider networks on a worldwide scale. TMN also has applicability in wireless communications, cable television networks, private overlay networks, and a host of other large scale, high bandwidth communications networks. TMN provides for integrating new multi-vendor equipment with legacy systems within a common network management structure. The TMN architecture integrates management, service, and accounting functions in order to achieve higher service quality, reduced costs, and faster product integration. TMN eliminates competitive barriers by demanding that manufacturers open up their equipment by supporting a common management architecture. With the worldwide TMN acceptance by telecommunications and wireless carriers, equipment manufacturers must support TMN in order to remain competitive. The scope of TMN managed areas includes: switching networks, transmission networks, ISDN, B-ISDN/ATM, data networks, and mobile networks.

The TMN relevant standards are documented in the ITU M.3000 Series: M.3000 and M.3010 for TMN, and X.701 for OSI Management. The TMN architecture in M.3010 is defined from three perspectives: a physical architecture and an information architecture based on the manager-agent concepts of OSI systems management, X.701; a functional architecture describing layering of TMN management functionality; and the application of architecture to the management of various technologies (described in the following documents: SDH networks in G.784, switching in Q.513, SS7 networks in Q.750, and ISDN in M.3600).

Where additional TMN application functionality beyond that provided by existing OSI Management standards is needed, it is built on existing OSI capabilities provided by the OSI CMIS, X.710. Such enterprise management services in turn are mapped onto associated application protocol data units defined in the OSI CMIP, X.711, for transfer across TMN interfaces.

10.3.2.6 Emerging Management Efforts for Multimedia Networks

The emerging network management standards and products are being developed to provide an open framework, core services, and unifying applications that integrate voice, data, and mixed media network environments across multiple vendors and locations and give customers sophisticated, comprehensive, enterprise-level network management capabilities. In this environment, it appears that the computer communication and telecommunications network standards organizations will allow the SNMP and CMIP network management protocols to coexist.

For instance, the ATM Forum has been working on a series of network management standards for configuration management, fault management, and performance management. The ATM Forum network management standardization focuses on the management information base (MIB) specifications, which define managed objects and associated attributes that are necessary to implement various management functions. The keys to an open network management platform are a common communications protocol and a common set of managed objects or information elements to facilitate monitoring and control of ATM network elements. These are realized through a standard MIB.

In this context, there are a large number of relevant MIBs. MIBs are based on simple network management protocol (SNMP) or common management information protocol (CMIP) standards. Besides The ATM Forum MIBs (SNMP and CMIP), there are MIBs defined by other standards bodies including the Internet Engineering Task Force (SNMP), TOG (CMIP), and ITU-T (CMIP). In addition, there are proprietary MIBs developed by vendors to manage their switches (primarily SNMP-based). Even though each standards body has specific objectives, there is some overlap between MIBs developed by different standards bodies. Often, users need a combination of various MIBs to meet their requirements. To manage ATM networks, it is important to understand the applicable MIBs, their purpose, scope and inter-relationships.

10.3.2.6.1 ATM Forum MIBs

As ATM technology goes across private networks and public networks, ATM network management has different perspectives depending on whether one is interested in managing the private or public networks or both. The ATM Forum has defined a generic model that encompasses both areas. Basically, the ATM Forum network management model defines five interfaces: M1, M2, M3, M4, and M5. Private ATM network management is addressed through M1 combined with M2. M1 is concerned with management of end user equipment connecting to either private or public switches, and M2 with management of ATM switches and networks. M3 is the link between private and public networks to exchange fault, performance and configuration information. M4 pertains to management of public ATM switches and networks. M5 supports interactions or exchange of management information between any two public networks.

10.4 System Quality

Implementations of IT infrastructure, systems and services should identify measures of quality that indicate levels of performance. Prior to initiating any IT implementation, initial planning to match and align the IT solution to support the organization’s functional missions is a crucial first step. That step should include measures of effectiveness for assessing resultant performance. During the subsequent development, implementation and operation of the IT system, the application of a consistent enterprise system quality framework is important. The prescribed set of measures include System Effectiveness, System Efficiency, System Characteristics, and System Behavior.

System Quality metrics can demonstrate the efficiency of the hardware and software infrastructure. Metrics are used in a wide range of activities – from validating acquisition effectiveness, to measuring central design performance, to allowing fine tuning of a system at the local level. The application of metrics across our diverse information systems represents a difficult task, one requiring focused management and special tools.

For all implementations, selecting the correct measurements, interpreting the data, and properly using the outcome is key to assessing performance. Prior to selecting any performance metrics it

is important to understand how to measure, what to expect from the measurement, the cost of the measurement, and how it fits into the enterprise-wide mission.

10.4.1 System Quality Concept

For warfighting readiness, performance of our IT infrastructure, and return on our IT investment, it is important that we have measures of performance. Measuring the quality of the Naval information infrastructure, in aggregate, is a formidable task. Effective measures have not been determined. The IT infrastructure is owned and maintained by multiple, independent organizations, making aggregation of measures very difficult. Accurate inventories and configuration management data are inconsistently maintained. There is an absence of financial benchmarks on which to base return on investment calculations. The remainder of this chapter establishes a framework upon which to gauge the effectiveness and efficiency of the DON enterprise information infrastructure. The system quality metrics that are introduced enable assessment of IT support of the mission and provide feedback to the system control methods that support system configuration, operation, and implementation.

The system should be continually examined under demanding operational scenarios to verify its operational performance. The system should be stressed through exercises covering at least these three scenarios:

- A logistics operation (e.g., Desert Shield)
- A tactical operation (e.g., Desert Storm)
- A natural disaster (e.g., Provide Comfort)

System quality data should be collected and retained for statistical and trend analysis.

The dimensions to System Quality are explained using a simple model illustrated in Figure 10-8:

System Effectiveness – Metrics and attributes that describe how well the IT infrastructure helps customers perform their mission objectives and tasks. These metrics and attributes also identify the responsiveness of the infrastructure to emerging requirements.

System Efficiency – Metrics and attributes that provide the system costs to develop, implement, operate and maintain as a function of mission effectiveness.

System Characteristics –Attributes that describe the static condition of systems or system components after implementation or reconfiguration.

System Behavior – Metrics and attributes that show how the collection of system components are responding to usage and the current situation.

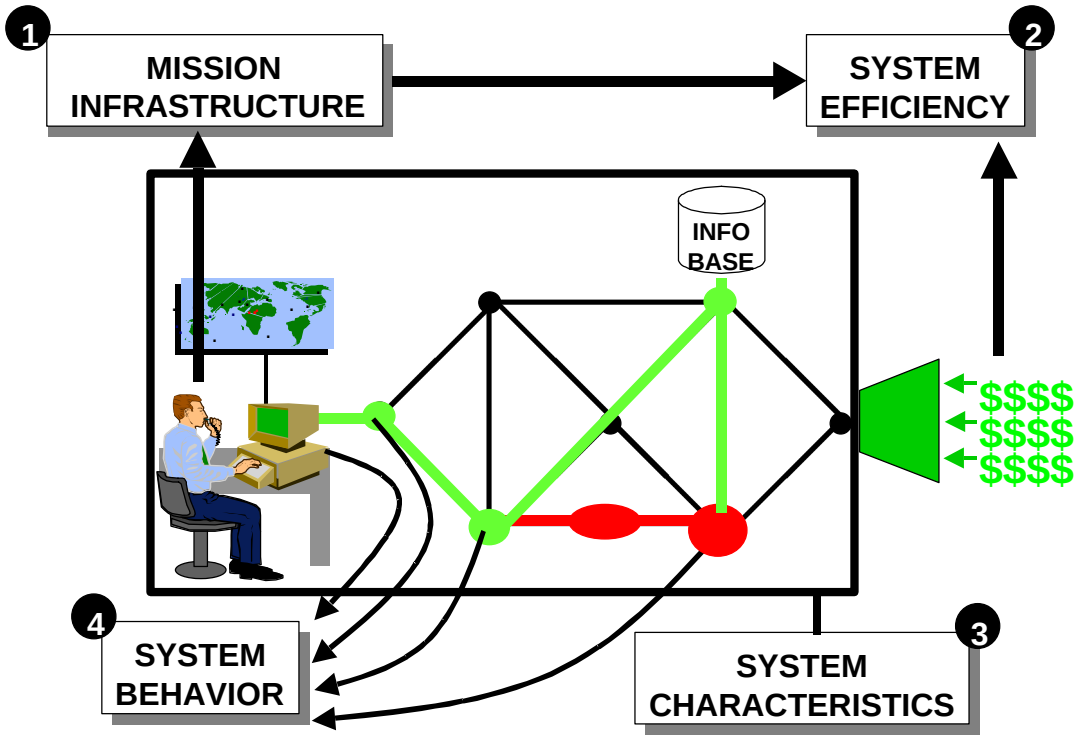


Figure 10-8. Systems quality dimensions

The Systems Characteristics dimension has a relationship with the three remaining dimensions. Varying the attributes of System Characteristics causes changes to System Behavior and System Efficiency (based on cost). These changes to System Behavior are further manifested in changes to System Effectiveness.

This model must be further developed to adequately measure quality on the complex system that comprises the DON enterprise information infrastructure. Of the four dimensions, System Effectiveness and System Efficiency can be measured independently of what is going on inside the individual Information System Domains (ISDs). System Behavior and System Characteristics are explained by events and data residing within each ISD; their measures can be obtained effectively only within an individual ISD, but any attempt to aggregate these rapidly gains complexity when crossing ISD boundaries.

However, System Behavior metrics, because of their ability to show response to operational conditions and system performance, must be aggregated to provide enterprise measures. The concept of coordinated ITSCs, with their enterprise management responsibilities and supported clientele help mitigate this complexity.

Infrastructure Effectiveness		**System Characteristics**	
System Performance		Block Diagram	BD
Suitability	SUIT	System Identifying Information	SII
Availability of Capability	AVC	Network Characteristics	NET
Vulnerability	VUL	Application Characteristics	APPS
Task Time	TT	Appliance Characteristics	APDV
Task Improvement	TI	Facility Characteristics	FAC
Capability Response	CR	Scalability	SCA
Information Quality		**System Behavior**	
Accuracy	ACY	Volume	VOL
Precision	PCN	Capacity	CAP
Error Rate	ER	Throughput	TP
Time-Late	TL	Throughput Rated	TP-R
Time Since Validation	TSV	Congestion	CG
Completeness	COMP	Blocking	BK
Duplication	DUP	Utility	UT
Accessibility Target	ACSY-T	Availability	Ao
Accessibility Actual	ACSY-A	Mean Time Between Failures	MTBF
System Efficiency		Mean Time to Repair	MTTR
Cost	COST	E-mail to No One	EMN
Total Cost of Ownership	TCO		
End-User Maintenance Cost	EUMC		
Subscriber Value	SV		
Net Subscriber Value	NSV		
Return on Investment	ROI		

Table 10-3. Dimensions of System Quality

Table 10-3 summarizes the system quality metrics that support the four dimensions – Infrastructure Effectiveness, System Efficiency, System Characteristics, and System Behavior. These metrics are described in the remainder of the chapter. Each of the four descriptions includes at least one summary table that follows the format of Table 10-4. The summary tables can be used by managers as work sheets to assess performance of these four dimensions.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Title	Abbreviation	Unit of Measure	Who performs the Measurement
Description or formula for computation			

Table 10-4. System Quality Metrics Summaries (format)

10.4.2 System Effectiveness

The formulation of relevant, quantitative, timely, and universally applicable metrics of mission effectiveness for application to information infrastructure is very challenging. Development of

these metrics is illustrated in Figure 10-9. Two tracks are shown, one that leads from the mission through organizational elements – functions, tasks and people; and the second that leads from the infrastructure through system elements – applications, networks and appliances. The first track must be understood to properly determine and apply the metrics obtained from the second track.

Appliances and people intersect to create the capabilities needed to accomplish the task. The figure shows the relationship between capabilities and requirements that feeds back to organizational functions and system applications. Capabilities lead to the following results: more information, better understanding, increased knowledge, greater productivity, good decisions, and proper directions as depicted at the bottom of the figure.

The infrastructure's contribution to producing the "Results" is measured by the System Performance and Information Quality. Both serve to enhance Infrastructure Effectiveness. The items under System Performance measure how well the system supports the task. The items under Information Quality measure the goodness of the system's product – information.

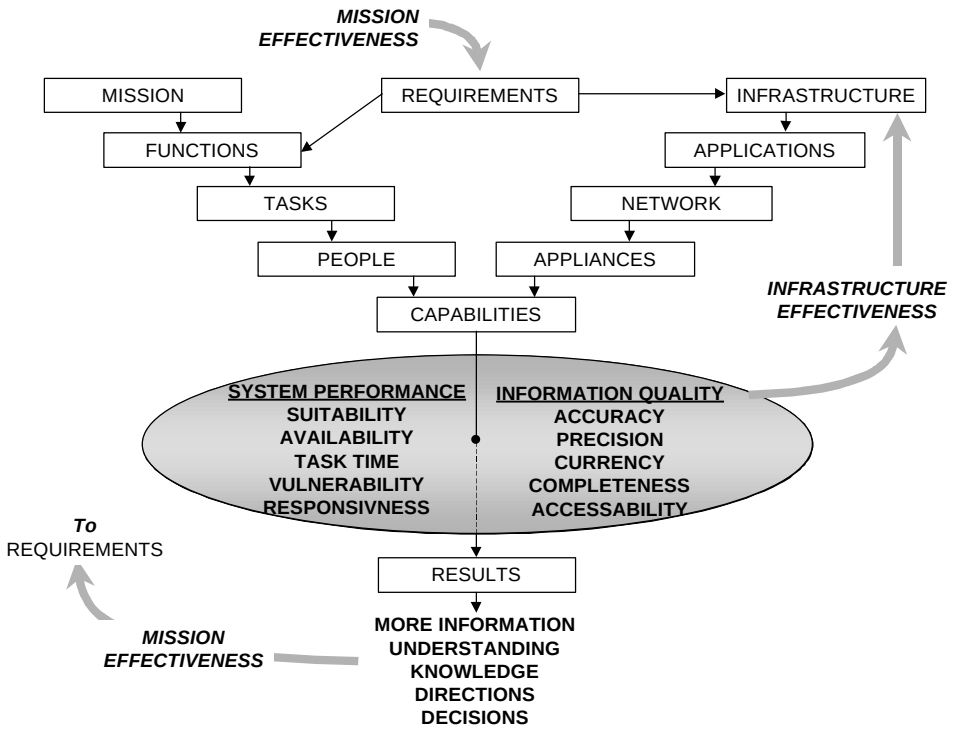


Figure 10-9. Relationship Between Mission and Infrastructure Effectiveness

10.4.2.1 System Performance

The measures of information system performance are as follows.

> **Suitability.** How well system capability matches the required task – "Is the system doing the right job?" The system does several jobs, therefore suitability (expressed as a percentage) will be the number of tasks supported over the number of tasks expected to be supported by the system subscriber.

Availability. How much of the time the system capability can be expected to be present when it is needed. It is the total sum of time that each system capability is operable divided by the product of elapsed time and number of system capabilities.

Vulnerability. The ability to deny a service or obtain unauthorized access to information. It is measured by a vulnerability assessment team on an intrusive, but harmless, basis and recorded as number of intrusions per week. Associated details must be recorded and tracked as well.

Task Time. The length of time taken to complete a common, standard task. This provides a measure of productivity and improvement. Productivity increases as less time is taken to complete a task, so that more tasks can be completed within a given time. Improvement in task times before and after a system upgrade can be used to determine a percent enhancement (or decrement). The challenge is in determining common standard tasks.

Capability Responsiveness. The length of time it takes for a system to adapt and provide new or altered capability based upon emergent subscriber requirements. The units of measure would likely be in days and should be averaged over all capabilities provided or upgraded.

Quantifying these measures hinges on defining the functional system capabilities and common standard tasks.

10.4.2.1.1 Defining Required Functional System Capabilities

As discussed in Chapter 2, the four core capabilities for the infrastructure are: (1) command LAN and standard client personal workstations, (2) distributed communications to dispersed forces, (3) wide area network communications to shore and garrison forces, and (4) basic network and information distribution services (BNIDS). Functional capabilities -- common operational picture, employment scheduling, repair parts tracking -- are predicated on these core capabilities. Fleet Commander-in-Chiefs (CINCs) and the Marine Force Commanders will define required functional system capabilities that need to be measured and tracked.

10.4.2.1.2 Defining Common Standard Tasks

Likewise, “common standard tasks” need to be identified and selected. Candidates should be tasks that are performed frequently and don’t require substantial research or innovation, but nevertheless are essential to the organization’s mission. A representative common standard task is the creation and ultimate delivery of a Casualty Reports (CASREPs).

The CASREP requires diagnosis of a broken component and research to collect information that is transcribed into a message. The message is sent to a group of common CASREP recipients as well as recipients that need to know the readiness status of the unit. Once the CASREP message is received by supporting units, action and coordination ensues to solve the problem. This common standard task could be supported by a system capability that replaces the CASREP message with a trouble ticket system. The casualty reporting task would remain common but the data entry and transfer method would change. The affected unit would enter the data directly into the CASREP database. The information would then be automatically posted or routed to the supporting commands that need to take action.

The functional system capabilities and the common standard tasks will be identified and selected as the ITSG matures.

10.4.2.1.3 Calculating Suitability Metrics

Each command should provide input to the ITSC to develop a list of tasks expected to be supported by the information infrastructure. Supported tasks over the total expected supported tasks is the command's suitability (percentage). The command's suitability will be updated monthly by the servicing ITSC. The ITSC should collect suitability values from each command, then calculate mean, median, mode, standard deviation, variance and extreme values for the region. Fleet and Global ITSCs should determine the same suitability statistics by echelon, geographic area, and platform type. These statistics should be calculated monthly and analyzed for trends. The resultant analysis should be used to guide and prioritize information technology implementation.

10.4.2.1.4 Calculating Capability Availability Metrics

Each command should help the ITSC identify important information system capabilities required for mission support — both organic (locally owned and operated) and remote. Capability examples include commercial items such as word processing or electronic mail as well as operational items such as automated message handling or common operational picture. ITSCs will maintain comprehensive lists of these functional capabilities. Capability outages, assessed locally or identified by client commands, will be tracked by the ITSCs. The availability of the command's information infrastructure (AVC) for the month is as follows:

$$\text{AVC} = \frac{\text{(NUMBER OF Capabilities) * (Elapsed Time) – Sum of elapsed time of capability outages}}{\text{(NUMBER OF Capabilities) * (Elapsed Time)}}$$

Servicing ITSCs should determine each command's monthly AVC. The ITSC should also collect AVC for the region and calculate mean, median, mode, standard deviation, variance and extreme values. Fleet and Global ITSCs should determine the same AVC statistics by echelon, geographic area, and platform type. Analysis of this data should be used to guide and prioritize information technology implementation.

10.4.2.1.5 Determining Vulnerability

Vulnerability (VUL) is determined by and ITSC vulnerability assessment team and is the number of penetrations achieved over a week. The vulnerability assessment team should frequently probe the information infrastructure with intrusive but harmless efforts to gain access or identify areas where disruption could occur to system devices from external sources.

The full description of the penetration method and associated system vulnerability should be recorded and tracked. The collection and analysis of these measures shall be highly restricted but provided as needed to information system managers and commanding officers so that corrective action can be taken.

VUL = Number of penetrations per week

Vulnerability data should be collated by systems and echelons. ITSCs should perform associated statistical and trend analysis.

10.4.2.1.6 Calculating Task Time

Common tasks identified by the command should be measured to determine the average time required to execute. The task time sampling frequency is at command discretion . Task times (TT) should be collected by the ITSC for performance of standard statistical. Task times should be calculated after system upgrades to determine task improvement (TI) with the following calculation:

$$\text{Task Improvement} = \frac{\text{Old Task Time - New Task Time}}{\text{Old Task Time}}$$

10.4.2.1.7 Determining Capability Responsiveness

To measure capability responsiveness the new requirement must first be validated and sponsored by the appropriate authority. Upon commitment of funding (if required) the clock starts and runs until the capability is satisfactorily delivered by the system developer. Capability Responsiveness (CR) is the elapsed time from funding to system implementation as defined by the system developer expressed in elapsed work days. The Global ITSC should calculate and maintain mean, median, mode, variance, standard deviation and extreme value analysis as well as trend analysis.

10.4.2.1.8 System Performance Summary

Table 10-5 provides a summary of system performance metrics for mission effectiveness discussed.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Suitability	SUIT	Percent	Command Consumer
$\text{SUIT} = \frac{\text{Number of Supported Tasks}}{\text{Number of Tasks Expected to be Supported}}$			
Availability of Capability	AVC	Percent	Command Consumer
$\text{AVC} = \frac{\text{(NUMBER OF Capabilities) * (Elapsed Time) – Sum of elapsed time of capability outages}}{\text{(NUMBER OF Capabilities) * (Elapsed Time)}}$			
Vulnerability	VUL	Events per week	ITSC
Determined value. Number of events per week with descriptions			
Task Time	TT	Time (minutes)	Command Consumer
Measured Value. The average amount of time that is takes to do a common standard task. Task must be specified for comparison with like tasks.			
Task Improvement	TI	Percent	Command Consumer
$\text{Task Improvement} = \frac{\text{Old Task Time - New Task Time}}{\text{Old Task Time}}$			
Capability Responsiveness	CR	Time (work days)	System Developer
Measured Value. Elapsed time from funding to capability delivery.			

Table 10-5. System Performance Metrics Summary

10.4.2.2 Information Quality

Information is the ultimate product of the information infrastructure. Measuring the quality of the product is essential to gauging the infrastructure's support to the mission. Information quality – accuracy, precision, and currency – measure the goodness of the individual information elements. Completeness, duplication and accessibility measure the goodness of information sets.

Accuracy. The probability that the value is correct. Expressed as a percent, it is calculated by dividing the total number of correct values by the total number of values. It can also be expressed as an error rate equal to the number of errors over the total number of values. It can also be a pure probability calculated through statistical methods.

Precision. The fidelity, granularity or relevance of the information. It is expressed with the same unit of measure as the data element itself as a plus or minus tolerance within which the value is accurate.

Currency. The elapsed time from the creation, discovery or validation of the information to the present time.

Completeness. The number of information elements in the information base as a function of the total number of information elements in the entire set. Completeness is expressed as a percentage.

Duplication. The percentage of duplicate data elements in the information set.

Accessibility. The degree in which the information stored or computed within the infrastructure is available to the target subscriber. The metric should be time measured from when a subscriber initiates a search until the time information retrieval starts. It measures the combination of subscriber training, information organization, and system response.

Of the measures, the information producer must measure accuracy, precision, and completeness. The ITSC may coordinate an independent assessment if requested by the subscribers. The subscriber, or ITSC representing a subscriber, measures timeliness and accessibility. The ITSC should also maintain statistics and trend analysis for each information set.

10.4.2.2.1 Determining Information Accuracy and Precision

Information accuracy and precision go together. The accuracy of the information is dependent upon the stated precision. For example, the phrase "drive a car to work" is less precise than, but no less accurate than "drive a Volvo to work."

The information manager calculates the information accuracy (ACY) by performing a periodic assessment of the entire data set. The percentage is derived by subtracting the number of incorrect data elements from the total and then dividing by the total to obtain the percentage. In lieu of counting the total number of data elements (as attached to a particular task or functionality), a statistical sample set can be used to obtain a 95 percent confidence level at the precision level determined by the information manager or producer.

Information that requires a very high level of accuracy can be measured as an error rate (ER), where ER is a ratio of errors to the total number of data elements.

Information precision in a range or set of values that describe the detail or fidelity of the information. This level of fidelity is often determined by the capability of a sensor. The precision should be varied as necessary to ensure the accuracy level does not drop below a selected value. Most information should be maintained at a precision level that keeps accuracy above 99.9 percent with the most accurate data having an error rate or less than one per million. Precision is measured as a tolerance (plus or minus from the expected value) or a range (he set that contains the expected value to include the value itself). Precision can be varied depending on the mission element.

Information accuracy and precision should be computed monthly and submitted to the ITSC.

10.4.2.2.2 Calculating Information Currency

Information currency is either time-late (TL) for dynamic information, or the elapsed time since validation (TSV) for static information. Time-late is the time difference between time of the discovery or data creation, and the present time. Elapsed time since validation is the difference between the present time and the last validation time provided by the information producer or manager.

10.4.2.2.3 Determining Information Completeness

Completeness is the percent of data elements present in the information base over the number of data elements in the complete set. The information producer or manager calculates information completeness (COMP) first by determining the complete set of data elements present. Completeness should be determined by information production commands on a periodic basis with assistance from the ITSCs.

10.4.2.2.4 Determining Information Duplication

Duplication (DUP) is a negative measure that provides an indication that data base management needs improvement. It is proposed in order to put the “completeness” measure in perspective since data duplication can make a data base appear to be more complete. Duplication is the number of repeated occurrences of unique data elements divided by the total number of data elements. Duplication should be determined by the information production commands as needed for internal quality control. If required by information consumers, an independent measure of duplication by the ITSC can be performed and tracked.

10.4.2.2.5 Calculating Information Accessibility

There are two metrics associated with accessibility: target accessibility (ACSY-T) and actual accessibility (ACSY-A). The information producer or manager determines target accessibility. The manager makes the information accessible based upon the level of training and security access of the target information consumer. Target accessibility equals the sum of the data query time and the system expected response time. Actual accessibility is equal to the elapsed time from the start of the search to the start of the information download.

The ITSC must determine the cause of excessive ACSY-A with possible solutions being a system tune or operator training. In the case of ACSY-A where information cannot be retrieved, the ITSC must determine if the information is even available, and if not, determine if system capability should be upgraded. In this case, ‘system performance’ measures would be used (system capability response).

10.4.2.2.6 Information Quality Summary

Table 10-6 provides a summary of information quality metrics for mission effectiveness discussed.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Accuracy	ACY	Percent	Producer Manager
$ACY = \frac{\text{Complete Number of Data Elements} - \text{Number of Incorrect Data Elements}}{\text{Complete Number of Data Elements}}$			
Precision	PCN	Units of Associated Information	Producer Manager
Determined value. Tolerance within which an information element value is expected to fall or the description of the set of items in which the information element value is contained.			
Error Rate	ER	Errors per number of elements (million)	Producer Manager
$ER = \frac{\text{Total Number of Errors in the Period of Time}}{\text{Total Number of Data Elements in the Period of Time}}$			
Time-Late	TL	Time (minutes)	Command Consumer
TL = Present Time - Data Time Stamp or Time of Event			
Time Since Validation	TSV	Time (days)	Command Consumer
TSV = Present Time - Time Stamp at Validation			
Completeness	COMP	Percent	Producer Manager
$COMP = \frac{\text{Number of elements present in the information base}}{\text{Total Number of information elements in the complete set}}$			
Duplication	DUP	Percent	Producer Manager
$DUP = \frac{\text{Number of duplicative data elements}}{\text{Total Number of information elements in the complete set.}}$			
Accessibility - Target	ACSY-T	Time (seconds)	Producer Manager
Measured Value. Elapsed time from start of an information query until the retrieval of the information as measured by the information producer or manager.			
Accessibility - Actual	ACSY-A		Command Consumer
Measured Value. Elapsed time from start of an information query until the retrieval of the information as measured by the information consumer or supporter.			

Table 10-6. Information Quality Metrics Summary

10.4.3 System Efficiency

Efficiency is the amount of effectiveness or productivity over the amount of resources (money or time) expended. This section focuses on financial resources (time resources are addressed under

mission effectiveness because reducing the response time is the force multiplier that information provides infrastructure to the mission.)

System efficiency is a universal focus addressed predominately by commercial industry and normally includes two primary measures — “Total Cost of Ownership” (TCO) and “Return on Investment” (ROI). Both TCO and ROI are difficult to measure within the DON — TCO because of the fractionated information system implementation and ROI because the DON does not use profit as the primary measure of “return”. TCO and ROI as applied to the DON are addressed in this section.

10.4.3.1 Total Cost of Ownership (TCO)

TCO includes aggregating costs over the enterprise and aligning the cost categories with the infrastructure management system. Using this alignment, costs that appear to be out of line with expected values can be quickly investigated and corrected. Figure 10-10 shows a method for organization, categorization and aggregation. The ITSCs should compile and aggregate their data at each echelon on a monthly and annual basis. The tables are divided into several sections. The upper section provides display of costs for upgrade, technology refreshment, or migration of the infrastructure. The bottom section contains the cost breakdown for operations, maintenance, and support.

10.4.3.1.1 End-User Maintenance Cost (EUMC)

The ITSC mission is to minimize the amount of time that end users spend solving their own problems, although at times it is unavoidable. Commands that care to report this measure can do so under the metric End-User Maintenance Cost (EUMC). The EUMC is equal to the hourly rate multiplied by the number of hours spent troubleshooting and repairing a system. This performance measure is often attributable to the amount of resources provided to the organization. In some cases, it may be more economical to let users repair their own problems. This measure provides a methodology to guard against potential shifts in cost from the supporter to the user after reductions in infrastructure support resources. Costs passed to the end user can be tracked so that resources can be managed to minimize the total cost.

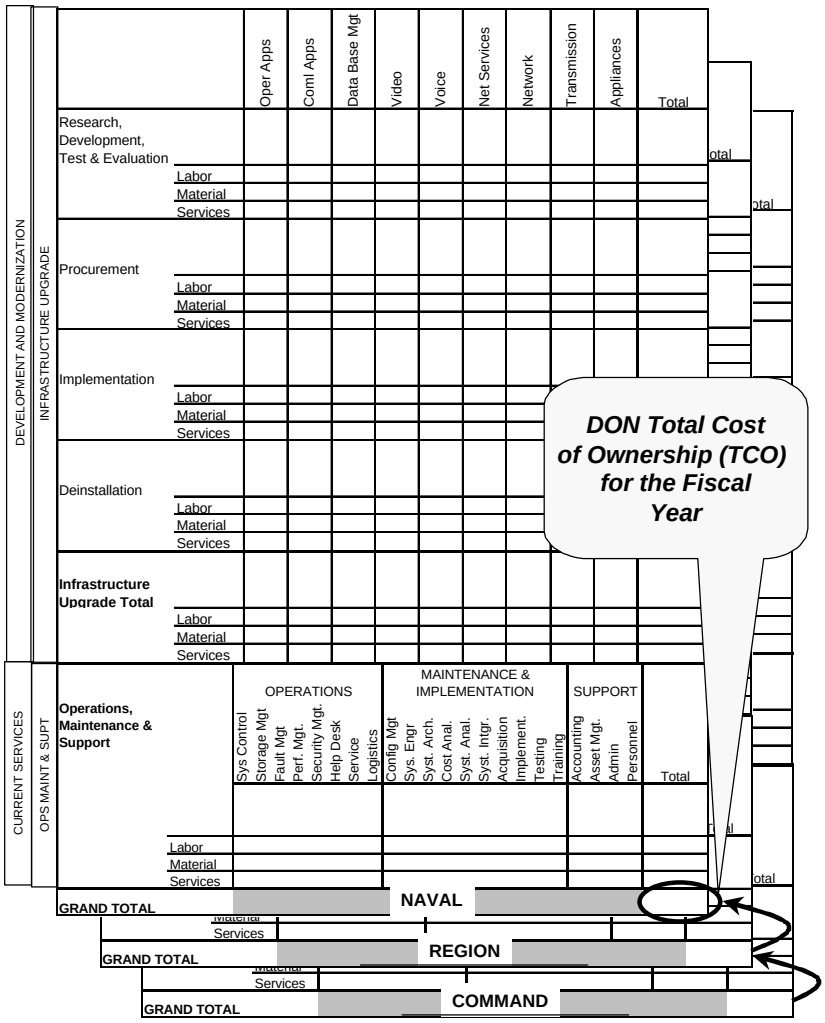


Figure 10-10. Aggregation of Costs to Provide the Total Cost of Ownership

10.4.3.1.2 Technology Refreshment and Infrastructure Upgrade Costs

In the above figure, infrastructure upgrade is broken down into four categories, with each subdivided into labor, material and services subcategories for greater detail. Across the top are columns that span the system component categories depicted in the rows of the enterprise management matrix, Figure 10-3. These costs are summed for each row and column over each echelon (command, region, Naval).

Research, Development, Test and Evaluation (RDT&E). The government has a significant role to play in researching and developing new information technologies. However, with the wealth of information technology resources in commercial industry, it is preferable to procure rather than develop. The focus has shifted from developing new technologies to testing and evaluating commercial products for integration into the Naval information infrastructure.

Procurement. Costs associated with systems, components and services to upgrade the infrastructure.

Implementation. Costs associated with the installation, integration, training, initial supply associated with the integration of a developed or procured system.

Deinstallation. Costs associated with the removal and disposal of obsolete or unneeded components.

10.4.3.1.3 Operations, Maintenance and Support

The bottom quarter of Figure 10-10 contains cost categories for Operations, Maintenance and Support (OM&S). As shown, the same cost categories of labor, material, and services are used as in the infrastructure upgrade section. The columns of the OM&S section match the enterprise management functions from the columns in Table 10-4.

10.4.3.2 Return on Investment (ROI)

TCO Section (10.4.2.1) and optional EUMC Section (10.4.2.2) provide the investment information needed for the ROI measure. Return can be measured using any of the system performance measures described in the mission effectiveness Section (10.4.1.1). The usefulness of ROI as a system efficiency measure greatly increases if a monetary value can be placed on system return. In a business sense, the customer provides revenue that generates a return (profit) after costs. The customers of the DON information infrastructure are the information consumer and information producer who rely on the infrastructure for receipt and delivery of information. Because the customer does not have to pay for any infrastructure benefit, an artificial value, related to mission effectiveness, can be assigned to the customer's beneficial use of infrastructure services.

10.4.3.2.1 Net Subscriber Value (NSV)

If a part of the infrastructure fails or if a service does not provide utility, a number of subscribers are impacted. The value of the information service to the subscriber is directly impacted by the time being spent using the system. The cost of downtime to a subscriber is the value of the subscriber's time lost due to non-availability of the system. Conversely, if the system shortens a task-time by allowing the user to more productively perform a task, then the value of the user's time gained is credited to the information system. To represent the value of the subscribers time (work-hours), the subscriber dollar value per hour (determined by the local comptroller) is multiplied by a utility factor and a mission criticality factor.

Subscriber Value (SV) = ($50) * Utility Factor * Criticality Factor

Where:

- $50 per hour is an arbitrary value chosen for the value of a subscriber's time
- Utility Factor is estimated percentage of time required to be spent on the service for the subscriber
- Criticality Factor is a percentage that expresses how critical a capability is relative to the command's mission.

Net Subscriber Value (NSV) = Sum of all associated Subscriber Values

ITSCs will assist Commanding Officers in establishing a utility factor and criticality factor for each information system capability and in determining the number of subscribers. ITSCs will

aggregate the subscriber values for each capability, each system and system component that comprise the information infrastructure.

As a result, the ITSCs not only have a monetary value of a capability, but also a monetary value for the down time of a system component. For example, the cost associated with an out of service client PC would be less than that of a server based on relative net subscriber value. Use of net subscriber value will be factored into architecture decisions when determining the degree of system component redundancy for fault tolerance.

The total ROI for the infrastructure is the net subscriber value for all system capabilities divided by the Total Cost of Ownership (TCO). The ROI can also be calculated for each of the Systems component capabilities. Add the applicable SV(s). Determine the percent these SV(s) are of the total NSV. Multiply the OM&S total by that percent to equal the approximate amount of OM&S associated with those capabilities.

10.4.3.2.2 System Efficiency Summary

Table 10-7 provides a summary of system efficiency metrics as discussed above.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Cost	COST	Dollars	Developer ITSC
Costs collected and collated by technology refreshment, operations, maintenance and support. Cost categories include labor, material, and services. For technology refreshment, subcategories include RDT&E, Procurement, Implementation, and Deinstallation. Cost also collated by technology and function.			
Total Cost of Ownership	TCO	Dollars	ITSC
Total aggregated costs of technology refreshment and operations, maintenance and support rolled up from commands into regions, regions into the Naval enterprise. Funds are also rolled up temporarily by month, quarter and fiscal year.			
End-User Maintenance Cost	EUMC	Dollars	Command Consumer
EUMC = Hourly Rate of the Subscriber * Time Spent Troubleshooting and Repairing the System			
Subscriber Value	SV	Dollars	Command Consumer
SV = Hourly Rate * Utility Factor * Criticality Factor			
Net Subscriber Value	NSV	Dollars per service or component	ITSC
NSV = Sum of all SVs associated with a service, capability, or component			
Return on Investment	ROI	Percent	ITSC
$ROI = \frac{\text{NSV for applicable capability, service system, or component (or any combination thereof)}}{\text{Net COST of applicable capability, service system, or component (or any combination thereof)}}$			

Table 10-7. System Efficiency Metrics Summary

10.4.4 System Characteristics

System characteristics measures are the controlling factors that determine the mission effectiveness and system efficiency measures discussed in the prior sections. System characteristics are simply the configuration of the information system domain.

10.4.4.1 System Configurations

The following is the minimum configuration items to be tracked by the ITSC to measure system characteristics. These items must be kept up-to-date.

System Block Diagram

System Identifying Information

- Domain Name
- IP Addresses
- ATM NSAP Addresses

Network Characteristics

- Number and Description of External Interfaces
  - WAN Service Providers
  - Communication Servers
  - Virtual Networks
- Network Topology
  - Network Diagram
  - Number and Description of Internal Network Nodes
  - Network Diameter expressed in Number of Nodes
  - Description of Cable Plant
  - Network Protocols Used

Application Characteristics

- Number and Description of Servers
  - Function
  - Processor(s)
  - Clock Speed
  - Memory
  - Storage
  - Operating System
  - Maximum Subscribers
- Commercial Application Software
  - Function(s)
  - Product
  - Vendor
  - Subscribers
  - License Information
  - Server Information
  - Maximum Subscribers

- Operational Application Software
  - Function(s)
  - Product
  - Developer
  - Sponsor
  - Subscribers
  - License Information
  - Server Information

Appliance Characteristics

- Number and Description of Computer Clients
  - Function
  - Processor(s)
  - Clock Speed
  - Memory
  - Storage
  - Maximum Subscribers
- Commercial Application Client Software
  - Function(s)
  - Product
  - Vendor
  - Operational Application Client Software
  - Function(s)
  - Product
  - Vendor
  - Number and Description of VTC Clients
  - Number and Description of Network Telephones

Facility Information

- Platform/Site Description
- Number of Buildings
- Location

10.4.4.2 Meshing Information System Domains

Information services and applications provided to a subscriber require an interwoven framework of networks, data sources and applications spanning several information system domains. As illustrated in Figure 10-11, the ITSCs will mesh information system domains as necessary to identify the system chains needed to achieve enterprise capability. Using this method, ITSCs will be able to compare system characteristics and system behavior with mission effectiveness and system efficiency.

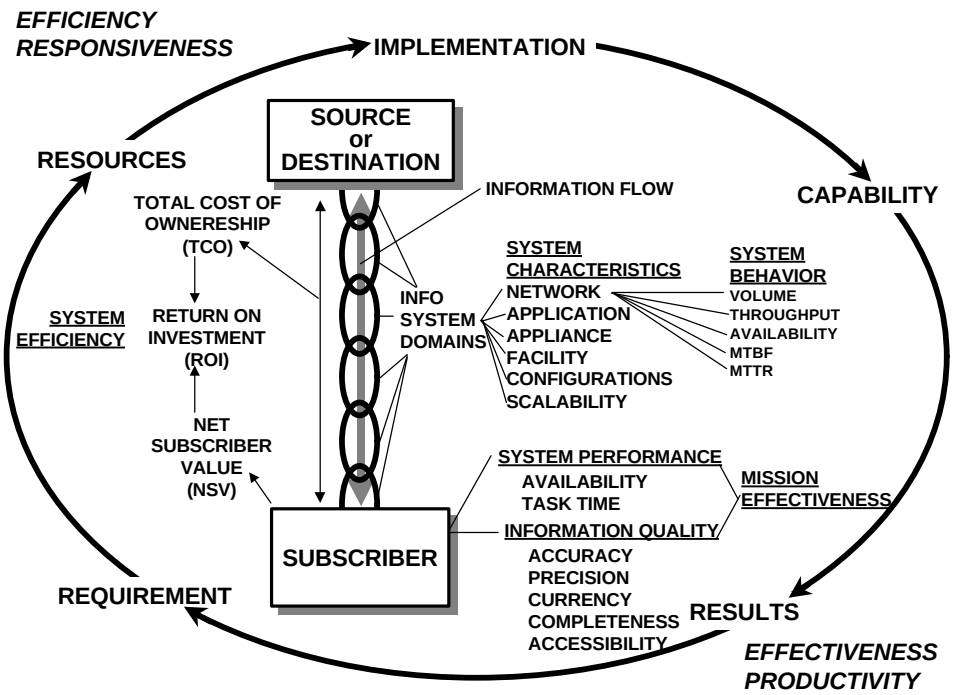


Figure 10-11. Summary of System Quality Measurements

10.4.4.3 Scalability

Scalability (SCA) is a measure of how easily a system can expand to meet an increased number of subscribers. For each operating system and software application associated with the capability, the maximum number of subscribers that an application or subsystem can support is tracked. For the chain of information systems associated with a system capability, or for an entire information system domain, the minimum value of all ‘maximum subscribers per application or subsystem’ becomes the scalability. In effect, scalability is the maximum number of users that can be supported.

Scalability is important to enterprise management because the Naval enterprise consists of nearly one million potential subscribers. Integrated information subsystems and components must be capable of meeting the full-scale requirements of the enterprise.

10.4.4.4 System Characteristics Summary

Table 10-8 provides a summary of system characteristics metrics as discussed above.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Block Diagram	BD	Diagram	ITSC
Block Diagram of each information system domain within an area of coverage.			
System Identifying Information	SII	Descriptive Data	ITSC
Command Name, Domain Names, IP Addresses, ATM NSAP Addresses, Staff Code Schema, E-mail Address Schema			
Network Characteristics	NET	Diagrams & Descriptive Data	ITSC
External Interfaces, Topology, Diagram, Nodes, Net Diameter, Cable Plant, Protocols			
Application Characteristics	APPS	Descriptive Data	ITSC
Servers, Commercial Server Software, Government Server Software, VTC Servers			
Appliance Characteristics	APDV (Appliance Devices)	Descriptive Data	ITSC
Computer Clients, Commercial Client Software, Government Client Software, VTC Clients, Network Telephones			
Facility Characteristics	FAC	Diagrams & Descriptive Data	Command Consumer
Platform/Site Description, Number of Buildings, Locations of Facilities, Floor Plans, Power			
Scalability	SCA	Determination	ITSC
SCA = Minimum of (Maximum Subscriber of All System Components)			

Table 10-8. System Characteristics Metrics Summary

10.4.5 System Behavior

The fundamental system behaviors necessary to track the health of the infrastructure are as follows:

Storage Volume (VOL). Bytes currently being stored by a node or system component. It should be determined on an periodic basis and tracked for trend analysis and compared against the current situation. System behavior is often a function of the volume of information that it contains. Systems operating near capacity often exhibit abnormal symptoms.

Storage Capacity (CAP). The maximum volume that a system component can handle.

Throughput (TP). The number of bits per second that are transmitted or processed by a system component.

Throughput Rating (TP-R). The maximum number of bits per second that can be processed or transmitted by the system component at the physical layer.

Link Congestion (CG). Physical throughput divided by throughput rating.

Blocking (BK). Percent of time that a circuit cannot be established due to capacity being reached at a node.

Link Utility (UT). Number of different users or services attempting to use the link in a given period of time.

Availability (Ao). The amount of time that a system component is operating in an up status over the total elapsed time.

Mean Time Between Failures (MTBF). The average elapsed time between failures of a system component.

Mean Time To Repair (MTTR). The average elapsed time from the failure of a system component until its return to operation.

E-mail to No One (EMN). The measure of network and server response by sending an e-mail to no one between any two sites. The e-mail will bounce due to “no addressee found” and be returned to sender. The elapsed time from transmission to receipt of the non-delivery is a good measure of network and server loading as well as system faults.

System behavior is most easily measured on a component-by-component basis using the metrics described above. System behavior and system characteristics information can be used to identify areas where infrastructure improvement is needed. The ITSCs must collect and aggregate system behavior metrics and perform statistical analysis to investigate improvements in system performance and identify potential problem causes. Network modeling and simulation can be used to predict system behavior based upon proposed alternative changes in system characteristics.

Table 10-9 provides a summary of system behavior metrics discussed above.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Volume	VOL	Bits	ITSC
Measured Value. Amount of bits currently present or stored in a system component or network node. For servers and computer clients this value can be expressed in bytes. Units must be specified.			
Capacity	CAP	Bits	ITSC
Value designated by the vendor, service provider or developer. Maximum amount of bits that can be present or stored in a system component or network node. For servers and computer clients this value can be expressed in bytes. Units must e specified.			
Throughput	TP	Bits per second	ITSC
Measured Value. Flow rate of processing rate of data. Can be physical or virtual (through compression)			
Rated Throughput	TP-R	Bits per second	ITSC
Value designated by the vendor or developer. Data rate or processing rate specified by the vendor, service provider or developer.			
Congestion	CG	Percent	ITSC
$CG = \frac{\text{Measured Physical Throughput on a Node or Link}}{\text{Rated Physical Throughput on a Node or Link}}$ Measurable by Network Analyzers or Circuit Analyzers			
Blocking	BK	Percent	ITSC
$BK = \frac{\text{Number of Calls or Circuits that get blocked due to lack of capacity on a switch}}{\text{Total Number of Calls or Circuits that are attempted. (measurable)}}$			
Utility	UT	Number per Minute	ITSC
UT = Number of users or services that attempt to use a system component over a period of time			
Availability	Ao	Percent	ITSC
$\frac{\text{Elapsed Time (month)} - \text{Down Time for a System Component or Object}}{\text{Elapsed Time (month)}}$			
Mean Time Between Failures	MTBF	Time (days)	ITSC
Calculated Value based on collected Data. Average lapsed time from one failure to the next for a system component or object. Important for trend analysis.			
Mean Time to Repair	MTTR	Time (hours)	ITSC
Calculated Value based on collected Data. Average lapsed time from failure to service return for a system component or object. Important for trend analysis.			
E-mail to No One	EMN	Time (seconds)	ITSC
Measured Value. Elapsed time from transmission of an e-mail to a non-existent address to receipt of the error notification from the destination e-mail server.			

Table 10-9. System Behavior Metrics Summary

10.4.6 Selection of Performance Metrics

Each of the metrics listed in sections 10.4.1 – 10.4.5 will be of varying degrees of utility to systems implementers and customers. Several concepts are useful in selecting which set of metrics to use from an enterprise organizational perspective.

10.4.6.1 IT Results Chain

The use of specific performance metrics should be aligned from the enterprise strategic plan via an IT/IM results chain. In other words, metrics should relate IT/IM outcomes to customer objectives, which are in turn related to enterprise program requirements. This helps one to focus on the metrics which truly support decision-making and program outcomes, and prevents optimization of individual customer results, to the detriment of the enterprise .

10.4.6.2 Balanced Scorecard

Performance metrics should be selected in such a way that they achieve a balance between both operational and strategic measures. Four generic goal areas include:

- Meeting the strategic needs of the enterprise
- Meeting the needs of individual operational users
- Addressing internal IT business performance (e.g., Total Ownership Cost; CDA performance; system metrics), and
- Addressing ongoing IT innovation and learning to achieve process improvement.

10.4.6.3 Targeted Measures

Organizations should match measures and performance results to the appropriate level of management/decision-making. These levels include DON, Regional, Command, and so forth. IT goals and measures should be included in IT performance improvement plans, and can even be tied to budgeting and procurement processes.

10.4.6.4 Comprehensive Measurement Capability

One should consider the way IT performance will be collected, analyzed, baselined, and benchmarked. One should select collection and analysis tools which will provide consistent indications of IT performance while automating the collection and analysis tasks as much as possible. The IT measurements and the process by which they are collected and analyzed should be periodically reviewed for appropriateness.

Note that these concepts are given as guidance on how to establish enterprise level performance measures. It is expected that in future releases of this ITSG, more detailed guidance will be provided on how to develop enterprise performance measurements and associated processes.

10.5 References

DOD Enterprise Management

Defense Information Systems Agency (DISA): Joint Defense Information Infrastructure Control Center Concept of Operations (DII CC CONOPS); 22 July 1997

Enterprise Management Metrics

Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investment; Exposure Draft; GAO/AIMD-97-163; General Accounting Office; http://www.gao.gov/policy/guidance.htm (Sep 97)

XSM

The Open Group (TOG) X/Open Systems Management, 6 July 1996; http://www.rdg.opengroup.org/public/pubs/catalog/t602.htm (24 May 1998)

Simple Network Management Protocol (SNMP)

Case (SNMP Research), Fedor, Schoffstell (Performance Management Inc.), Davin (MIT); "Simple Network Management Protocol (SNMP)" (IETF Standard 15/RFC-1157); May 1990: ftp://ftp.isi.edu/in-notes/rfc1157.txt (24 May 1998)

Rose (Performance Management Inc.), McCloghrie (Hughes LAN Systems) "Structure and Identification of Management Information for TCP/IP-based Internets" (IETF Standard 16/RFC-1155) , May 1990; ftp://ftp.isi.edu/in-notes/rfc1155.txt (24 May 1998)

Rose (Performance Management Inc.), McCloghrie (Hughes LAN Systems); "Concise MIB Definitions" (RFC-1212) March 1991; ftp://ftp.isi.edu/in-notes/rfc1212.txt (24 May 1998)

McCloghrie (Hughes LAN Systems), Rose (Performance Management Inc.); "Management Information Base for Network Management of TCP/IP-based internets: MIB-II" (IETF Standard 17/RFC-1213),March 1991, ftp://ftp.isi.edu/in-notes/rfc1213.txt (24 May 1998)

Waldbusser (Carnigie Mellon) , "Remote Network Monitoring Management Information Base", (RFC 1757) February 1995; ftp://ftp.isi.edu/in-notes/rfc1757.txt (24 May 1998)

Simple Network Management Protocol version 2 (SNMPv2)

Case (SNMP Research Inc.), McCloghrie (Hughes LAN Systems), Rose (Dover Beach Consultant Inc.), Waldbusser (Carnigie Mellon); Introduction to version 2 of the Internet-standard Network Management Framework (RFC 1441) April 1993RFC 1441, Simple Network Management Protocol Version 2, May 1993

Common Management Information Protocol

International Organization for Standardization (ISO) standard: ISO/IEC 9596-1/ITU-T X.711 "Common Management Information Protocol (CMIP)Specification;" 23 May 1998; http://www.iso.ch/cate/d29698.html (24 May 1998)

Remote Network Monitoring Version 2 (RMON2)

Waldbusser (INS), "Remote Network Monitoring Management Information Base Version 2 using SMIv2" (RFC 2021); January 1997; ftp://ftp.isi.edu/in-notes/rfc2021.txt (24 May 1998)

Biermen (Cisco), Iddon, (Axon Networks Inc.); “Remote Network Monitoring MIB Protocol Identifiers” (RFC 2074): January 1997 ftp://ftp.isi.edu/in-notes/rfc2074.txt (24 May 1998)

Web Based Enterprise Management (WBEM)

Free Range Media, Inc.; “Draft Proposal, WEBM” Version 0.4, 16 July 1996 http://wbem.freerange.com/new/wbem/obsm.htm (24 May 1998)

Intel Inc.; “Web Based Enterprise Management, Simplifying and Reducing the Cost of PC Ownership”; http://www.intel.com/managedpc/wbem/; (24 May 1998)

Duri, Weber (IBM Zurich Research Laboratory); “Webbin’ CMIP,” http://www.igd.fhg.de/www/www95/proceedings/posters/43/index.html (Jan 1998)

Desktop Management Interface (DMI)

Desktop Management Task Force (DMBF); Desktop Management Interface (DMI) Draft Proposal, DMI Version 2.0,29 March 1996 http://www/dmtf.org/ (24 May 1998)

ATM Forum Network Management Specification

ATM Forum web site: http://www.atmforum.com (30 May 1998)

International Telecommunications Union (ITU) Standards

International Telecommunications Union – Telecommunications (ITU-T); M.3000 Series of Recommendations on Telecommunications Management network (TMN) October 1997 http://www.itu.int/itudoc/itu-t/rec/m.html (24 May 1997)

Index

1

100BaseFX 112
100BaseT 79, 112

8

802.11 77, 110, 120, 144

A

Acquisition 4, 5, 231, 243, 244, 282, 315, 4
Address resolution protocol 136
Addressing137, 139, 141, 142, 148, 160, 274, 2, 3, 7, 13, 40
Air filter 91, 92
Aircraft 30, 75, 98, 104, 142, 165
Airflow 91
AMON 117, 119
API116, 170, 174, 190, 208, 211, 217, 218, 219, 220, 227, 228, 268, 270, 291, 292, 294, 295, 300, 302
ARP 118, 136, 139, 146, 147
Ashore 3, 23, 28, 124, 125, 161, 235, 302, 303
ATM12, 13, 14, 22, 24, 25, 26, 49, 53, 54, 89, 105, 106, 107, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 121, 122, 124, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 147, 148, 150, 302, 304, 306, 307, 309, 18, 19, 34, 37, 42
ATM NICs 115
ATM switches 53, 89, 114, 115, 118, 119, 140, 19
Authentication43, 44, 45, 47, 48, 49, 51, 55, 56, 57, 175, 179, 204, 215, 17
Available bandwidth 22, 103, 242

B

Best practices 3, 5, 8, 12, 39
BGP-4 140
BLACK Cables 87
BNIDS16, 149, 150, 151, 152, 159, 160, 232, 238, 286, 289, 7, 24
Border Gateway Protocol Version 4 140
BUS 118
Bypass switches 112, 305

C

Cable26, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 98, 99, 103, 105, 109, 115, 120, 122, 1, 4, 10, 18, 34, 37
Cable entry 91
Cable Plant 76, 88, 89, 98, 99, 34, 37
CAD/CAM 202, 253, 269
Calendaring 288, 289, 291, 300
Category 5 76, 78, 83, 109, 115, 123
CDDI 112
CFM 91
CIDR 138, 139, 147
Classical IP 115, 116, 136, 144
Classical IP over ATM 136, 144
Classless Inter Domain Routing 138, 139
Client/server4, 5, 160, 174, 209, 213, 218, 297, 298, 300
Client/Server 4, 5, 202
Clinger-Cohen Act 3, 233, 235, 237, 282
Commercial SATCOM 94, 128, 130
Conduit 87
Cooling 91, 98
Cooperative Work Applications 288, 295
Copper cable 76, 79, 89, 109, 113
CPU190, 193, 194, 196, 197, 202, 204, 206, 207, 208, 209, 224
Crossovers 82
Cyrix 194, 202, 203

D

DAS 115, 121
Data administration234, 235, 238, 261, 263, 266, 276, 279, 280
Data modeling 234, 239, 277, 279
Decommissioning schedule 79
Defense in Depth 42, 43
Deployed1, 3, 16, 27, 28, 57, 58, 104, 105, 124, 137, 142, 180, 198, 210, 246, 7, 9, 10
Desktop ATM 113
Desktop Management Task Force 17, 42
DHCP 138, 139, 141, 142
Digital signature 57, 61, 64, 65, 67, 68, 69, 70, 164
DII COE4, 38, 192, 209, 210, 227, 264, 282, 287, 288, 310, 313
Direct Sequence Spread Spectrum 120
Directory services7, 149, 150, 160, 162, 163, 165, 167, 180, 187, 213, 214, 291, 7
Distance Vector Multicast Routing Protocol 140, 147
Distributed computing 37, 208, 212, 312
DMS47, 61, 62, 154, 156, 157, 158, 159, 163, 164, 165, 166, 167, 169, 188, 192
DMTF 12, 13, 17

DNS 47, 141, 150, 160, 161, 162, 168, 187, 217
Document Management 271
DON CIO BOR 2, 3, 9, 10
DQPSK 120
Drop Cable 78, 84, 109
DVMRP 139, 140
DVS 306

E

Edge devices 115, 119
EGP 138, 139, 140
ELANs 117
Electric load analysis 92
Electrical Components 97
Electronic Forms 298
E-mail15, 16, 21, 22, 36, 50, 53, 54, 56, 57, 58, 60, 61, 63, 69, 114, 115, 131, 137, 138, 148, 150, 151, 152, 153, 154, 155, 156, 158, 159, 160, 163, 164, 165, 166, 167, 168, 169, 175, 177, 180, 182, 186, 205, 241, 272, 291, 297, 300, 22, 37, 38, 39
Emulated LANs 117
Encryption40, 48, 49, 53, 54, 56, 58, 59, 64, 65, 67, 70, 120, 303, 309
Ethernet25, 106, 108, 109, 110, 111, 112, 114, 115, 116, 117, 118, 119, 133, 136, 144, 146, 307, 309
Ethernet NICs 115

F

Fans 90, 91, 92, 224
Fast Ethernet106, 108, 109, 110, 111, 112, 114, 118, 119, 148
Fault tolerance 111
FDDI106, 110, 111, 112, 114, 115, 116, 118, 119, 136, 144, 146, 147, 309
FDDI concentrators 118
FDDI NICs 115
FDDI switches 111, 118
FDDI wrap times 116
Fiber Optic Cable 78, 82
Fiber Optic Cable Plant 78
File Transfer Protocol 138, 172, 188
Fire protection 96
Firewall24, 25, 44, 45, 46, 47, 48, 50, 52, 54, 170, 312, 5
Fixed configuration 119
Flammability 79
Floating neutral 92, 101
FOCP 78, 79, 81, 82, 83, 84, 86, 88
Frequency Hopping Spread Spectrum 120
FTP 45, 47, 50, 138, 172, 173, 188, 280

G

GDS 162
GFSK 110, 120
Gigabit Ethernet 108, 110, 112
GOTS 49, 192, 207, 278, 281, 288, 289, 310
Graphics22, 89, 174, 176, 179, 194, 219, 239, 242, 245, 246, 247, 250, 253, 288, 289, 290, 293, 294, 299
Ground 32, 75, 93, 97, 104, 105, 126, 17
Grounded neutral 92
Guidance1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 15, 16, 20, 21, 29, 30, 33, 34, 35, 36, 37, 39, 45, 49, 53, 54, 55, 59, 64, 66, 75, 86, 88, 97, 103, 104, 109, 119, 120, 133, 139, 151, 153, 160, 164, 168, 193, 201, 212, 220, 221, 222, 223, 235, 237, 253, 275, 285, 288, 292, 297, 311, 1, 3, 6, 12, 40, 41

H

HIPERLAN 110, 120
HTML98, 99, 145, 147, 148, 174, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 201, 221, 227, 228, 229, 243, 244, 245, 246, 247, 282, 313, 17, 41, 42
HTTP45, 47, 53, 138, 173, 174, 175, 179, 181, 183, 210, 17
HVAC 93, 98, 253

I

ICMP 47, 136, 139, 146
IEEE 802.10 117, 144
IEEE STD 802.11 120, 121
IGMP 136, 139, 147
IGP 138, 139, 140
IISP 114, 148
Imaging 242, 293, 294
Imaging systems 293
Infrared 120
Infrastructure2, 3, 4, 5, 6, 7, 8, 11, 12, 15, 16, 17, 18, 19, 21, 22, 23, 27, 28, 29, 31, 32, 34, 41, 43, 49, 60, 61, 64, 79, 85, 88, 103, 104, 106, 107, 131, 133, 136, 137, 150, 151, 152, 154, 164, 165, 171, 182, 224, 231, 240, 259, 273, 286, 287, 288, 297, 1, 2, 3, 4, 9, 11, 12, 19, 20, 21, 22, 23, 24, 25, 27, 30, 31, 32, 33, 37, 38
Interconnection box77, 78, 80, 81, 82, 83, 84, 85, 86, 87, 88
Interconnection boxes77, 80, 81, 82, 83, 84, 85, 86, 87, 88
Interconnectivity 2, 3
Interface21, 31, 106, 112, 113, 115, 116, 122, 127, 128, 138, 139, 141, 145, 147, 148, 170, 172, 174, 177, 190, 195, 197, 198, 208, 213, 219, 220, 221, 222, 223, 225, 226, 227, 228, 239, 249, 257, 270, 272, 291, 298, 312, 5, 9, 15, 17, 42
Interfaces12, 92, 165, 166, 174, 190, 197, 220, 227, 228, 229, 288, 34, 37
International Standards Organization 13, 103, 149, 313
Internet4, 12, 13, 15, 22, 24, 28, 44, 49, 56, 57, 71, 72, 73, 103, 121, 124, 125, 131, 133, 134, 135, 136, 138, 139, 140, 143, 146, 147, 153, 155, 159, 160, 162, 166, 167, 170, 172, 173, 174, 175, 176, 177,

179, 182, 183, 184, 186, 187, 188, 191, 214, 216, 245, 267, 269, 270, 283, 307, 311, 312, 19
Internet Protocol28, 71, 103, 124, 125, 133, 134, 135, 136, 139, 146, 155, 173, 214
Interoperability1, 2, 3, 11, 14, 15, 17, 18, 20, 29, 34, 35, 36, 39, 49, 56, 57, 76, 103, 104, 111, 113, 116, 124, 127, 128, 134, 137, 140, 156, 158, 168, 173, 189, 191, 192, 195, 205, 208, 209, 211, 216, 219, 231, 232, 233, 234, 235, 238, 258, 259, 261, 263, 264, 265, 266, 268, 269, 273, 274, 275, 276, 278, 285, 287, 288, 289, 297, 301, 302, 303, 304
Intranet23, 27, 28, 29, 44, 45, 48, 52, 53, 54, 183, 267, 269, 270
IP 25, 45, 47, 48, 49, 51, 52, 53, 54, 71, 72, 90, 103, 115, 116, 117, 118, 121, 125, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 146, 147, 148, 150, 160, 173, 187, 188, 214, 304, 309, 310, 34, 37
IPSEC 49, 50, 71
IPX 110, 134, 137
ISDN83, 121, 122, 123, 124, 148, 303, 304, 305, 306, 307, 308, 309, 310, 18
ISO13, 37, 103, 109, 133, 144, 149, 162, 172, 176, 187, 189, 200, 214, 217, 219, 220, 224, 227, 228, 243, 245, 246, 247, 248, 250, 252, 253, 254, 266, 267, 268, 270, 294, 313, 10, 13, 14, 15, 41
ITSC31, 32, 77, 80, 81, 125, 134, 139, 142, 153, 154, 155, 159, 5, 8, 9, 10, 11, 15, 16, 17, 25, 26, 27, 28, 30, 33, 34, 37, 39

J

JAVA 311
JTA 3, 4, 11, 12, 16, 235, 237, 266, 276, 16

L

LAN16, 22, 24, 25, 26, 27, 29, 39, 53, 59, 105, 106, 107, 109, 111, 112, 115, 117, 119, 120, 134, 135, 140, 144, 148, 170, 197, 198, 204, 210, 241, 280, 301, 304, 305, 306, 307, 309, 310, 11, 24, 41
LAN Emulation 115, 119, 148
LANE 115, 116, 118, 136, 148
Latency 23, 28, 30, 111, 112, 142
LEC 121, 123, 124
LECS 118
LES 118
Line conditioners 92
Line Conditioning 92, 98
Line of Sight 27, 105, 125, 131, 132, 146
Local breakout boxes 82
Local cable 78, 85, 86

M

MAN 24, 25, 27, 28, 29, 105, 122, 6
Mandatory 35, 282
Mesh 85, 86, 109, 35
Messaging15, 162, 163, 165, 166, 167, 168, 169, 173, 188, 217, 218, 242, 291, 293, 297, 300
MIPS 194, 206, 208
Modular 28, 90, 119
MPOA 116, 136, 148

N

Native ATM 116
Network Layer 135
Network news 16, 185, 186, 297, 7
Network-Centric Environment 4
NIC 115, 116, 161, 203
NICs 115, 120

O

Obtaining IP Addresses 137, 148
OMG 212, 216, 227, 229, 269
Open Shortest Path First 138, 140, 147
Open System 4, 5, 12, 20, 37, 103, 149, 15
Open systems 13, 14, 199, 297, 298, 300
OpenAir 2.4 110, 120, 121
operating system8, 18, 36, 40, 54, 55, 60, 135, 142, 144, 160, 168, 171, 172, 173, 177, 189, 190, 192, 197, 204, 205, 206, 207, 208, 209, 210, 211, 212, 215, 216, 267, 269, 311, 4, 17, 36
Operating System13, 21, 54, 56, 72, 190, 192, 196, 203, 208, 209, 210, 211, 220, 227, 228, 34
OS40, 55, 190, 193, 194, 196, 206, 208, 209, 210, 211, 219, 221, 223, 224, 227, 256
OSPF2 139, 140

P

Patch Panel77, 78, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 91
Pentium 194, 202, 203, 206, 208, 211
PKI 43, 60, 61, 62, 63, 151, 159, 164, 166, 173
PNNI 110, 113, 114, 118, 138, 139, 140, 141, 148
Point-to-Point 129, 134, 136, 147
POSIX 13, 170, 207, 210, 211, 212, 220, 227, 228, 4
POTS 79, 121, 307, 309
PPP 25, 129, 134, 136, 137, 139, 147
Project Management 289, 315
proprietary12, 56, 57, 105, 114, 116, 120, 125, 129, 141, 163, 165, 172, 177, 200, 207, 212, 214, 216, 270, 274, 291, 293, 303, 304, 19
Proprietary Network Layer Protocols 137
Public Key Infrastructure60, 64, 151, 159, 164, 166, 173, 180

Q

Quality of Service 111, 135, 142, 309

R

Racks 85, 86, 90, 91, 92
RDBMS 89, 267, 268, 269, 313
Reconfiguration 113, 114, 144
Reconfiguration time 114
RED Cables 87
RED/BLACK Installation Guidance 87, 98
Redundancy 86, 113, 114
Redundancy Techniques 113
Redundant fibers 86
Remote Access Services 151, 172
RFC71, 72, 73, 115, 116, 136, 138, 139, 140, 144, 146, 147, 161, 167, 173, 175, 186, 187, 188, 41, 42
RIP 139, 140
RISC 194
RMON 90, 117, 118, 119, 171, 172, 12, 13, 16, 17
RMON2 90, 118, 15, 17, 41
ROI 6, 22, 30, 32, 33
Routers22, 23, 25, 28, 29, 51, 52, 53, 106, 107, 111, 119, 136, 139, 140, 144, 7
Routing18, 25, 51, 53, 117, 119, 133, 136, 138, 139, 140, 141, 142, 150, 166, 271, 272, 298, 301
Routing Information Protocol 140
Routing Protocols 140
RTP 138, 147, 178, 179
Ruggedized racks 90

S

SAS 115
SATCOM16, 27, 28, 93, 94, 100, 101, 105, 124, 125, 126, 127, 128, 145, 7
Satellite16, 27, 28, 93, 98, 100, 101, 105, 126, 127, 128, 129, 145, 7
Scalability 12, 113, 137, 193, 197, 205, 206, 36
Scheduling170, 211, 224, 288, 289, 291, 300, 306, 5, 24
Scope4, 10, 13, 18, 76, 133, 212, 233, 240, 254, 276, 277, 278, 288, 292, 297, 307, 1, 3, 9, 10, 18, 19
Shielded Twisted Pair 77, 78
Shipboard24, 30, 32, 75, 78, 79, 80, 82, 84, 85, 86, 88, 89, 90, 91, 92, 93, 94, 96, 101, 104, 107, 112, 113, 114, 119, 137, 303, 6
Shipboard AC power 92
Shock Isolation 92, 98
Shore27, 28, 32, 75, 79, 80, 82, 84, 85, 122, 126, 137, 148, 159, 165, 303, 304, 305, 6, 17, 24
SME 3
SMT 114, 118
SNMP48, 90, 117, 118, 119, 171, 172, 12, 13, 15, 16, 17, 18, 19, 41
SONET 26, 105, 106, 109, 110, 113
Spacecraft 104
Spanning Tree 114, 116, 118, 144
Spare fibers 86
Spreadsheet 245, 289
Standards1, 3, 4, 5, 8, 9, 10, 11, 12, 13, 14, 16, 24, 25, 33, 35, 36, 37, 49, 62, 63, 65, 67, 68, 70, 71, 73, 75, 88, 96, 98, 99, 100, 109, 120, 125, 126, 127, 128, 131, 144, 145, 146, 147, 161, 175, 187, 195, 196, 197, 199, 224, 225, 226, 227, 229, 244, 246, 247, 249, 250, 251, 253, 255, 256, 257, 259, 276, 277, 280, 283, 307, 309, 310, 313, 314, 2, 11, 42
STP 78
Subject Matter Expert 3
Susceptibility to kinking 78
System Quality 2, 19, 20, 22, 26, 29, 33, 36, 37, 39
System Specific Cable 78

T

Tactical16, 28, 132, 146, 192, 228, 255, 256, 257, 274, 278, 281, 306
TAFIM 222, 223, 228, 235, 237, 266, 276, 282
TCO 168, 22, 30, 31, 32, 33
TCP25, 52, 53, 117, 133, 134, 135, 137, 138, 142, 146, 160, 172, 174, 175, 187, 188, 203, 210, 212, 214, 215, 304, 305, 41
TCP/IP25, 117, 133, 134, 142, 172, 174, 203, 210, 212, 214, 215, 304, 305, 41
Telephony 13, 26, 105, 288, 300, 301, 302
Temperature rise 91
TEMPEST 87, 98, 305
Test procedure 78
Throughput106, 111, 112, 113, 116, 117, 119, 130, 195, 241, 37
TMN 12, 15, 18, 42
toxicity 79
Transport Layer 134, 137
Trunk 77, 80, 86, 88
Trunk Cable 77, 80, 86

U

UDP 53, 138, 160, 187, 188, 215
UNI 110, 113, 115, 118, 147
Unshielded Twisted Pair 76, 78
Upgrade funding availability 79
UPS 92, 97, 98, 101
User Datagram Protocol 138, 215
UTP 76, 77, 78, 79, 81, 84, 109, 110, 112, 123

V

Virtual LANs 117, 118
VPN 22, 24, 44, 45, 48, 49, 50, 52, 53, 54, 59, 60
VTC5, 8, 121, 122, 123, 133, 135, 288, 303, 304, 305, 306, 6, 7, 35, 37

W

WAN22, 24, 25, 26, 27, 28, 29, 39, 46, 50, 51, 105, 106, 107, 111, 112, 113, 121, 122, 124, 134, 135, 143, 144, 197, 241, 304, 309, 6, 34
WBEM 89, 172, 13, 15, 16, 17, 42

Web Browser 174, 175, 177, 182
Webserver 175, 210, 267
Wireless 76, 77, 110, 119, 120, 121, 132, 144
Wireless ATM 121
Word Processing 115, 242, 243, 271, 286, 289, 25
Workflow 271, 298
Workflow management 298
WWW54, 58, 59, 61, 164, 175, 176, 177, 210, 244, 278

X

X.40015, 47, 153, 156, 158, 163, 164, 165, 166, 167, 187, 188, 291
X.50047, 61, 155, 156, 158, 159, 162, 163, 164, 165, 167, 169, 173, 187
X.700 4, 5, 6, 13, 14, 15
X/Open 13, 116, 162, 207, 210, 211, 212, 227, 13, 41

Z

Zone 44, 46, 50, 51, 52, 53, 54, 170

Appendix A - Acronym List

3DES	Triple DES
ABR	Available Bit Rate
ACE	Automatic Calling Equipment
ACSY-A	Actual Accessibility
ACSY-T	Target Accessibility
ACY	Information accuracy
ADNS	Automated Digital Network System
ADSL	Asymmetric Digital Subscriber Line
ALE	Automatic Link Establishment
AMON	ATM Monitoring
Ao	Availability
AOE	Fast Combat Support Ship
AOR	Area of Responsibility
AOR	Replenishment Oiler (ship class)
API	Application Programming Interface
ARG	Amphibious Ready Group
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
AVC	availability of the command's information infrastructure
BAN	Base Area Network
BPCS	Base, Post, Camp, Station
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol (version 4)
BK	Blocking
BLII	Base Level Information Infrastructure
BNIDS	Basic Network and Information Distribution Services
BOGSAT	Bunch-Of-Guys (or Gals or both) Sitting Around a Table
BONDING	Bandwidth On Demand Interoperability Group
BPR	Business Process Reengineering
bps	bits per second
BRI	Basic Rate Interface
BUFR	Binary Universal Format for Representation
BUS	Broadcast/Unknown Server
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance
CA	Certification Authority
CAD	Computer-aided design
CADM	C4ISR Core Architecture Data Model
CADRG	Compressed Arc Digitized Raster Graphics
CALS III	Computer-aided Acquisition and Logistics Support
CAP	Channel Access Protocol
CAP	Storage Capacity
CASE	Computer Aided Systems Engineering
CASREP	Casualty Report
CATV	Cable Television
CBC	Cipher Block Chaining
CBR	Constant Bit Rate
CBS	Commission for Basic Systems
CCTV	Closed Circuit Television
CDDI	Copper FDDI
CDMA	Code Division Multiple Access
CG	Guided Missile Cruiser
CG	Link Congestion
CGI	Common Gateway Interface
CGM	Computer Graphics Metafile
CIB	Controlled Image Base
CIDE	Communication Information Data Exchange
CIDR	Classless Inter Domain Routing
CINC	Commander in Chief
CINCLANT FLT	Commander in Chief, U.S. Atlantic Fleet
CINCPACF LT	Commander in Chief, U.S. Pacific Fleet
CIO	Chief Information Officer
CKM	Constructive Key Management
CLEC	Competitive Local Exchange Carrier
CMC	Common Messaging Call

CMIP Common Management Information Protocol
CNET Chief of Naval Education and Training
CNSG Commander Naval Security Group
CO Central Office
CODEC Coder Decoder
COE Common Operation Environment
COI Community of Interest
COMP information completeness
CONOPS Concept of Operations
CONUS Continental United States
CORBA Common Object Request Broker Architecture
COTS Commercial Off-the-Shelf
CPE Customer Premise Equipment
CPS Certification Practices Statement
CR Capability Responsiveness
CRLS Certificate Revocation Lists
CSD Circuit Switched Data
CSTA Computer Supported Telecommunications Applications
CSU/DSU Customer Service Unit/Digital Service Unit
CTI Computer telephony integration
CTTA Certified TEMPEST Technical Authority
CUDA Comprehensive Utilities for Data Administration
CV Aircraft Carrier
CVN Aircraft Carrier (Nuclear)
DAC Discretionary Access Control
DAP Directory Access Protocol
DART Data Analysis and Reconciliation Tool
DAS DISN ATM Services
DBDB Digital Bathymetric Database
DBMS Database Management System
DCE Data Communications Equipment
DD Destroyer
DDDS Defense Data Dictionary System
DDG Destroyer (Guided Missile)
DEF Data Exchange Format
DES Digital Encryption Standard
DHCP Dynamic Host Configuration Protocol
DII COE DII Common Operating Environment
DII Defense Information Infrastructure
DIICC DII Control Center
DISA Defense Information Systems Agency
DISC DREN Intersite Services Contract
DISN Defense Information Services Network
DMA Defense Mapping Agency (now NIMA)
DMI Desktop Management Interface
DMS Defense Messaging System
DMTF Desktop Management Task Force
DMZ Demilitarized Zone
DN ISDN Directory Numbers
DNC Digital Nautical Chart
DNS Domain Name System
DON CIO Department of Navy Chief Information Officer
DON Department of the Navy
DPPDB Digital Point Positioning Data Base
DQE Data Quality Engineering
DREN Defense Research and Engineering Network
DS Digital Service
DSA Digital Signature Algorithm
DSA Directory Server Agents
DSCS Defense Satellite Communication System
DSL Digital Subscriber Line
DSS Decision Support System
DSS Digital Signature Standard
DSSS Direct Sequence Spread Spectrum
DSV-G Defense Video Service - Global
DTE Data Terminal Equipment
DTED Digital Terrain Elevation Data
DTOP Digital Topographic Data

DVMRP Distance Vector Multicast Routing Protocol
DWTS Defense Wideband Transmission System
ECTF Enterprise Computer Telephony Forum
EDI Electronic Data Interchange
EDMS Electronic Document Management Systems
EGP Exterior Gateway Protocol
EHF Extremely High Frequency
EIA Electronic Industry Association
ELAN Emulated LAN
EMI Electromagnetic Interference
EMN E-mail to Nobody
ER Error rate
ETSI Escuela Tecnica Superior de Ingenieros
FC Fiber Channel
FCC Federal Communications Commission
FCP Fleet Communications Package
FDBM Functional Database Managers
FDDI Fiber Data Distributed Interface
FDMA Frequency Division Multiple Access
FFG Frigate (Guided Missile) (ship class)
FHSS Frequency Hopping Spread Spectrum
FIPS Federal Information Processing Standard
FIWC Fleet Information Warfare Center
FOCP Fiber Optic Cable Plant
FOICB Fiber Optic Interconnection Box
FTP File Transfer Protocol
FWSEB Force Warfare Systems Engineering Board
Gbps Giga (billion) bits per second
GBS Global Broadcast System
GCC Global Control Center
GCCS Global Command and Control System
GCCS-M GCCS - Maritime
GCSS Global Combat Support System
GIF Graphics Interchange Format
GIS Geographic information system
GKS Graphical Kernel System
GMF Ground Mobile Forces
GNI Global Network Initiative
GOSC Global Operations and Security Center
GOTS Government Off-The-Shelf
GPS Global Positioning System
GRIB Gridded Binary
HDSL High Speed Digital Subscriber Line
HF High Frequency
HFC Hybrid Fiber/Coax
HiPPI High Performance Parallel Interface
HMMO HyperMedia Managed Object
HMMS HyperMedia Management Schema
HTML HyperText Markup Language
HTTP HyperText Transfer Protocol
IAB Internet Architecture Board
IATO Interim Authority To Operate
ICMP Internet Control Message Protocol
ICOM Inputs, Controls, Outputs and Mechanisms
IDEF Integration Definition for Function Modeling
IER Information Exchange Requirement
IETF Internet Engineering Task Force
IGES Initial Graphics Exchange Specification
IGMP Internet Group Multicast Protocol
IGP Interior Gateway Protocol
IITMS Integrated Information Technology Management System
ILEC Incumbent Local Exchange Carrier
IM Information Management
IM/IT Information Management/Information Technology
IMAP4 Internet Message Access Protocol Version 4

IMETS	Integrated Meteorological System
IMUX	Inverse Multiplexor
INFOSEC	Information Security (per DISA)
INFOSEC	Information System Security (per NIS)
INMARSAT	International Maritime Satellite
Intelsat	International Telecommunication Satellites
IOC	Initial Operating Capability
IP	Internet Protocol
IPSEC	Internet Protocol Security
IPT	Integrated Product Team
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISD	Information System Domain
ISDN	Integrated Services Digital Network
ISO	International Organization for Standards
ISO/OSI	International Organization for Standards/Open Systems Interconnect
ISD	Information System Domain
ISP	Internet Service Provider
ISSP	Information System Security Program
IT	Information Technology
IT21	Information Technology for the 21st Century
ITMRA	Information Technology Management Reform Act (Clinger-Cohen)
ITOC	Information Technology Outreach Center
ITSC	Information Technology Service Center
ITSDN	Interim Tactical Standard Data Network
ITSG	Information Technology Standards Guidance
IVR	Interactive Voice Response
IXC	Inter Exchange Carrier
JDIICC	Joint DII Control Concept
JIEO	Joint Interoperability and Engineering Organization
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JMCIS	Joint Maritime Command Information System
JMTK	Joint Mapping Toolkit
JPEG	Joint Photographic Expert Group
JTA	Joint Technical Architecture
JTAPI	Java TAPI
JTDLMP	Joint Tactical Data Link Management Plan
JTIDS	Joint Tactical Information Distribution System
JV 2010	Joint Vision 2010
JWICS	Joint Warfighter Intelligence Communications System
kbps	kilo (thousand) bits per second
KG/KIV	Key Generator (Crypto devices)
L2P	Layer-to-Layer Protocol
LAN	Local Area Network
LANE	LAN Emulation
LCC	Local Control Center
LDAP	Lightweight Directory Access Protocol
LDR	Low Data Rate
LEC	LAN Emulation Client
LEC	Local Exchange Carrier
LEO	Low Earth Orbit
LHA	Amphibious Assault Ship (General Purpose)
LISI	Levels of Systems Interoperability
LPD	Low Probability of Detection
LPD	Transport, Dock (ship class)
LPI	Low Probability of Intercept
LSD	Landing Ship Dock (ship class)
LWD	Littoral Warfare Data
MAC	Media Access Control
MAGTF	Marine Air-Ground Task Force
MAN	Metropolitan Area Network
MAPI	Messaging Application Programming Interface
MBONE	Multicast Backbone
Mbps	Mega (million) bits per second
MC&G	Mapping, Charting, and Geodesy
MCM	Mine Counter Measures
MCU	Multi-point Control Units

MD5 Message Digest-5
MDR Medium Data Rate
METOC Meteorology and Oceanography
MEU Marine Expeditionary Unit
MFI Multi-Function Interpreter
MIB Management Information Base,
MIC Message Integrity Check
MIDS Management Information Data System
MIL-HDBK Military Handbook
MIL-STD Military Standard
MIME Multipurpose Internet Mail Extension
MLS Multi-level Security
MLSF Mobile Logistics Support Force
MODEM Modulator Demodulator
MOSPF Multicast Open Shortest Path First
MPEG Motion Picture Experts Group (version 1)
MPEG2 Motion Picture Experts Group version 2
MPOA Multiprotocol Over ATM
MPP Multilink PPP
MROC Military Required Operating Capability
MS Message Store
MTA Message Transfer Agent
MTBF Mean Time Between Failures
MTTR Mean Time To Repair
MUA Message User Agent
NAC Network Access Controller
NAVAIR Naval Air Systems Command
NAVSEA Naval Sea Systems Command
NC Network Computer
NCTAMS Naval Computer and Telecommunications Area Master Station
NECC Navy EHF Communications Controller
NES Network Encryption System
NIC Network Information Center
NIC Network Interface Card
NID Network Intrusion Device
NIF Network Intrusion Filter
NIPRNET Non-secure IP (Internet Protocol) Router Network
NITFS National Imagery Transmission Format Standard
NITSC Naval Information Technology Service Center
NIWA Naval Information Warfare Activity
NMF Network Management Foundation
NNTP Network News Transport Protocol
NOC Network Operations Center
NSA National Security Agency
NSTISSAM National Security Telecommunications and Information Systems Security Advisory Memorandum
NSV Net Subscriber Value
NT1 ISDN Network Termination1 Device
NTP Network Time Protocol
NVI Naval Virtual Intranet
NWTDB Naval Warfare Tactical Database
OA Office Automation
OC Optical Carrier
OCE Open Collaboration Environment
OCR Optical Character Reader
ODA/ODIF Office Document Architecture/Office Document Interchange Format
ODBC Open Data Base Connectivity
ODMG Object Database Management Group
OM&S Operations, Maintenance and Support
OMG Open Management Group
OODBMS Object-oriented database management systems
OQL Object Query Language
ORB Object Request Broker
OSI Open Systems Interconnect
OSPF Open Shortest Path First
PAID Procedures, Applications, Infrastructure, and Data
PBX Private Branch Exchange
PC Personal Computer

PCAT Personal Computer Access Tool
PCN Information precision
PEO Program Executive Office
PEX PHIGS Extension to X
PGP Pretty Good Privacy
PHIGS Programmer's Hierarchical Interactive Graphics System
PHY Physical Layer
PKCS Public Key Cryptography Standards
PKI Public Key Infrastructure
PM Program Manager
PNNI Private Network to Network Interface
POP3 Post Office Protocol Version 3 (example of MS)
POSIX Portable Operating System Interface definition
POTS Plain Old Telephone Service
PPBS Planning Programming Budget System
PPP Point to Point Protocol
PRI Private Rate Interface
PSK Phase Shift Keying
QDR Quadrennial Defense Review
QoS Quality of Service
RA Registration Authorities
radio-WAN Radio-based Wide Area Network
RADSL Rate Adaptive Digital Subscriber Line
RBOC Regional Bell Operating Companies
RCC Regional Control Center (now ROSC)
RDA Remote Data Access
RDBMS Relational Database Management Systems
RDT&E Research, Development, Test and Evaluation
RF Radio Frequency
RFC Request for Comment
RIP Routing Information Protocol
RITC Regional Information Technology Center
RMA Reliability, Maintainability, Availability
RMA Revolution in Military Affairs
RMON Remote Network Monitoring (version 1)
RMON2 Remote Network Monitoring (version 2)
ROI Return on Investment
ROSC Regional Operations and Security Center
RPF Raster Product Format
RS Recommended Standard (from EIA)
RSVP Resource Reservation Protocol
RTP Real-time Transport Protocol
Rx Receive
S/MIME Secure MIME
SABI Secret and Below Initiative
SAG SQL Access Group
SATCOM Satellite Communications
SBU Sensitive but Unclassified
SCI Sensitive Compartmented Information
SCV Subscriber Capability Value
SDD Secure Data Device
SDSL Symmetric Digital Subscriber Line
SGML Standard Generalized Markup Language
SHA Secure Hash Standard
SHF Super High Frequency
SIDR Secure Intelligence Data Repository
SIPRNET Secret IP (Internet Protocol) Router Network
SITE Shipboard Information, Training and Entertainment
SLIP Serial Line IP
SME Subject Matter Expert
SMI Structure of Management Information
SMT Station Management
SMTP Simple Message Transfer Protocol
SMWS System Management Work Station
SNMP Simple Network Management Protocol

SNMPv1 Simple Network Management Protocol, Version 1
SNMPv2 Simple Network Management Protocol, Version 2
SNMPv3 Simple Network Management Protocol, Version 3
SNTP Sneaker Net Transfer Protocol
SOE Standard Operating Environment
SONET Synchronous Optical Network
SPAWAR Space and Naval Warfare Systems Command
SPDL Standard Page Description Language
SPID ISDN Service Profile Identifiers
SPPTP Secure Point-to-Point Tunneling Protocol
SQL Structured Query Language
SSA Software Support Activity
SSC Software Support Center
SSL Secure Socket Layer
SSN Submarine (Nuclear)
ST Snap-twist
STE Secure terminal Equipment
STEP Standard Tactical Entry Points
STOW Synthetic Theater of War (network)
STP Shielded Twisted Pair
STU Secure Telephone Unit
SUIT Suitability of the command's information infrastructure
TAFIM Technical Architecture Framework Information Management
TAPI Microsoft/Intel Telephony API
TAWDS Tactical Automated Weather Distribution System
TCC Total Capability Cost
TCO Total Cost of Ownership
TCP Transmission Control Protocol
TDMA Time Division Multiple Access
TEMPEST Electromagnetic Emissions Susceptibility (not an acronym)
TI Task Improvement
TIA Telecommunications Industry Association
TL Time-Late
TOG The Open Group
TP Throughput
TP-R Throughput Rating
TRM Technical Reference Model
TSAPI AT&T/Novell Telephony Services API
TT Task time
TTL Time to Live
Tx Transmit
UARNOC Unified Atlantic Region Network Operations Center
UBR Undefined Bit Rate
UDI Unrestricted Digital Information
UDP Universal Datagram Protocol
UHF LOS Ultra High Frequency - Line of Sight
UHF Ultra High Frequency
UHF-DAMA Ultra High Frequency - Demand Assigned Multiple Access
UJTL Universal Joint Task List
UNI User to Network Interface
USCG US Coast Guard
USENET A global Internet-based bulletin board service
USMC US Marine Corps
USMTF United States Message Text Format
UT Link Utility
UTP Unshielded Twisted Pair
UVMap Urban Vector Map
VBR-NRT Variable Bit Rate - Non Real Time
VBR-RT Variable Bit Rate - Real Time
VIC Vendor-Independent Calendaring
VIM Vendor-Independent Messaging
VITD Vector Product Interim Terrain Data
ViViD Voice Video and Data Contract
VIXS Video Information Exchange System
VLAN Virtual LAN
VMap AD Vector Map Aeronautical Data
VMap Vector Map
VOL Volume
VPF Vector Product Format
VPN Virtual Private Network

VRML Virtual Reality Modeling Language

VTC Video Teleconferencing

VTS Vessel Traffic System

WAN Wide Area Network

WBEM Web-Based Enterprise Management

WDM Wave Division Multiplexing

WDP Web Drop and Pickup

WGS-84 World Geodetic System 84

WHEC High Endurance Coast Guard Cutter

WMEC Medium Endurance Coast Guard Cutter

WMO World Meteorological Organization

WPB Coast Guard Patrol Boat

WVS+ World Vector Shoreline Plus

WWW World Wide Web

XAPIA X.400 API Association

XMN X/Open Systems Management

Appendix B - Glossary

The official telecommunication glossary for the DON ITSG is Federal Standard 1037C of 1996 which can be found at:

http://glossary.its.bldrdoc.gov/fs-1037/

FED STD 1037C is maintained by the U.S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunications Sciences, Boulder, CO. It has over 5800 entries and is a compilation of the following glossary documents.

MIL-STD-188-120, Glossary of Telecommunication Terms (1996)
FED-STD-1037, Glossary of Telecommunication Terms (1980)
NTIA-SP 79-14, Fiber Optics Glossary (1979)
NBS Handbook 140, which became EIA-440A, & IEEE 812, Fiber Optics Glossaries (1979-1980)
FED-STD-1037A, Glossary of Telecommunication Terms (1986)
FED-STD-1037B, Glossary of Telecommunication Terms (1991)

To complement FED STD 1037C, the following references also provide glossaries on computer and information processing terms:

http://www.itsi.disa.mil/glossary.html

http://www.ora.com/reference/dictionary

http://wombat.doc.ic.ac.uk/foldoc/index.html

The following terms are particularly germane to the DON ITSG.

Activity Model A graphic representation of a business process that exhibits the activities and their interdependencies that make up the business process to any desired level of detail. An activity model reveals the interactions between activities in terms of inputs and outputs while showing the controls paced on each activity and the types of resources assigned to each activity. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Accreditation A certification made by the a designated approval authority that a sites information system meets all required security standards and has authority to operate within the established guidelines.

Activity Model, (As-Is) An activity model that portrays how a business process is currently structured. It is used to establish a baseline for subsequent business process improvement actions or programs. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Activity Model, (To-Be) An activity model that results from a business process redesign action or program. The TO-BE model shows how the business process will function after the improvement action is implemented. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Architecture An organized framework consisting of principles, rules, conventions, and standards that serve to guide development and construction activities such that all components of the intended structure will work together to satisfy the ultimate objective of the structure. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2dEdition, Electronic Version)

Architecture A unified set of rules for developing standard products. I.e. a shared vision. (Chorales, Dimities N. Systems Architecture & Systems Design, McGraw, 1989)

Appliance With regard to information technology, any device by which an end user receives, processes, or transmits information on the selected media. Information appliances include computers, telephones, televisions, video teleconferencing equipment and the like. It is also the hardware component that is part of an information appliance suite such as a mouse, keyboard, or video screen. In the three-tiered application architecture, these devices are referred to as “presentation clients”. It includes the hardware, software, and associated peripherals that the operator uses to interface with the system. This includes computer clients, servers, printers, telephones, video teleconferencing (VTC) equipment, and associated software.

Application A collection of system components that supports a particular task or function. It includes end-to-end, multi-media communications as well as information management and decision support capability. Distributed computing applications are normally built using a three-tiered architecture consisting of the application server, data server, and presentation clients which may be physically on a single device or on multiple devices connected by a network. Communication applications normally involve a minimum of two communication devices connected by the network.

Application Data Element A data element used in an automated information system. (An application data element may, or may not, be a standard data element.) (OPNAVINST 9410.6)

Application Server A server that hosts operational or commercial software applications supporting a network, command or community of interest.

Approved Product A product that has been certified for use by a competent authority for a particular application or mission and for a specified operational environment.

As-Is Model A model that represents the current state of the organization modeled, without any specific improvements included. Can be either an ACTIVITY MODEL or RULEMODEL (contrast TO-BE MODEL). (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Attribute A property or characteristic of an entity. An attribute has a name and a value. Attributes are used to identify and distinguish between entities and to provide descriptions of entities. Attributes are named with singular generic nouns. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Available Product A product that meets the requirement.

Basic Network and Information Distribution Services The very basic network services and the most fundamental applications that all platforms and activities need, independent of their command mission and operating environment. BNIDS include network packet or circuit delivery, domain name service, directory service, electronic mail (e-mail), web service, file storage and transfer, network time service and network news service.

Best Practice A practice that is considered to be the most effective and efficient.

BNIDS Basic Network and Information Distribution Services. See above.

Business Rule Model (Data Model) A graphical representation of an organization's information and data assets expressed in terms of entities and relationships. Relationships are called business rules because they enable or constrain business actions. Rule models, like activity models, have AS-IS and TO-BE representations. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Certification A statement attesting an interface has been verified as performing to a specification, standard, or other published document (JTC3A Circular 9002).

Client-Server Any network-based software system that uses client software to request a specific service, and corresponding server software to provide the service from another computer on the network.

Cognizant Agency The responsible agency for producing information or data.

Command Correspondence Information or direction issued by the commanding officer or his designated representative that carries the official intent and authority of the command.

Commercial Applications Commercial software programs or commercial procured hardware that satisfies a specific purpose.

Computer An electronic contrivance that solves problems and does complicated calculations by processing data according to prescribed programmed instructions and then produces and/or retains the outcome of these processes.

Control Center See DII Control Center.

Corporate Information Management (CIM) The DoD effort to apply computing, telecommunications, and information management capabilities effectively in the accomplishment of the Department mission.

Currency Regarding information is either time-late for dynamic information, or the elapsed time since validation for static information. Time-late is the time difference between time of the discovery or data creation, and the present time. Elapsed time since validation is the difference between the present time and the last validation time provided by the information producer or manager.

Data Symbols representing instances, or occurrences, of specific meanings in the real world. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Data Administration(DAdm) That function of the organization which oversees the management of data across all functions of the organization, and is responsible for central information planning and control. (NBS Special Pub 500-149)

Data Administrator (DAd) A person or group that ensure the utility of data used within an organization by defining data policies and standards, planning for the efficient use of data, coordinating data structures among organizational components, performing logical database design, and defining data security procedures. (NBS Special Pub 500-152)

Data Category All data sets necessary to define a functional category, e.g., sensors. The number of data sets per category is based on specific data file record capabilities.

Data Content What goes in a data element as defined by the data element definitions and formats.

Data Dictionary A specialized type of database containing metadata that is managed by a data dictionary system; a repository of information describing the characteristics of data used to design, monitor, document, protect, and control data in information systems and databases; and application of a data dictionary system. (FIPS Special Pub500-152)

Data Element (1) A named unit of data. It can be used to describe the atomic level of data, whether computerized or manual, as viewed by the user.

(2) In database usage, a named identifier of the entities and attributes that are represented in a database. (American National Standards Institute (ANSI) X.3.138-1988 and FIPS Pub 156 Definition)

(3) In Joint Service usage, a basic unit of information having a meaning and subcategories (data items) of distinct units and values.

Data Element Standards The standardization and management of data element definitions, formats, content, and relationships between data elements.

Data File All data categories which relate to a composite object, e.g., ship, aircraft.

Data Fill The actual data (or lack of) in the data element fields.

Data Integration Agreement of data messages between senders and receivers, enforced by business rules. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Data Merging Combining data from multiple digitized sources. A prerequisite to computer data merging is the up-front Deconfliction of data element standards and database structure.

Data Model (Business Rule Model) A graphical representation of an organization's information and data assets expressed in terms of entities and relationships. Relationships are called business rules because they enable or constrain business actions. Data models, like activity models, have AS-IS and TO-BE representations. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Data Server A server that hosts a data base management system or information base that supports applications, queries, or reports via a network for a command and/or community of interest.

Data Set A group of data elements that collectively describe a composite object, e.g., platform, weapon, sensor, installation, or other object.

Data Set Structure A representation of the logical relationships that exist among the data elements comprising the data set. The data set structure defines unique identifiers within the data set, subordinate relationships, repeating or multi-valued occurrences, and coded or constrained elements.

Data Standard (also called **Standard Data**) A data element that has been through a formal analysis to reach agreement on its name, meaning, and characteristics, as well as its relationship to other standard data elements. Much like a common language, data standards enable processes and their supporting information systems to be integrated across functions, as well as within them, and improve the quality as well as the productivity of enterprise performance.(DEPSECDEF Memo of 13 Oct 1993, "Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement)

Data Standardization The process of reviewing and documenting the names, meanings, and characteristics of data elements so that all users of the data have a common shared understanding of it.

Data standardization is a critical part of the DoD Data Administration Program, managed under DoD Directive 8320.1. Data administration is the function that manages the definition and organization of the Department's data. (DEPSECDEF Memo of 13 Oct. 1993, "Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement)

Data Translation The computer conversion of one data element format into another format; e.g., truncation of the 30 character ship name field into a 26 character field for use by a hardware and/or software constrained system.

Database A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data. (FIPS Special Pub 11-3)

Defense Data Dictionary System (DDDS) The database administered by the DISA Center for Information Management for managing the submission, review, and approval of DoD standard data elements.)

Defense Information Infrastructure (DII) The web of communication networks, computers, software, data bases, applications, weapon systems interfaces, data security services, and other services that meet the information processing and transport needs of DOD users across the range of military operations. It encompasses: (1) sustaining base, tactical, DOD-wide, information systems, command, control, communication, computer and intelligence (C4I) interfaces to weapon systems; (2) the physical facilities used to collect, distribute, store, process, and display voice, data and imagery; (3) the applications and data engineering tools, methods and processes to build and maintain the software that allow Command and Control (C2), Intelligence, Surveillance, Reconnaissance, and Mission Support users to access manipulate, organize and digest proliferating quantities of information; (4) the standards and protocols that facilitate interconnection and inter-operation among networks; and (5) the people and assets which provide the integrating design, management and operation of DII, develop the applications and services, construct the facilities and train others in DII capabilities and use. [DODD 5105.19-1991]

A seamless web of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing and transport needs of DOD users in peace and in all crises, conflict, humanitarian support, and wartime roles. [DII Master Plan 1.0]

Developmental Data Set A preliminary data set dealing with reference data from a Functional Database Manager that is still undergoing testing and coordination.

DII Control Center Center that performs independent and integrated missions supporting communications and information systems. These systems include LAN, MAN, and WAN management, help desks, technical control facilities, facility control offices, and network management centers. Provides essential operational support to the sustainment of the DII. [JDIICC CONOPS]

Draft Data set A data set derived from the registration of existing Tactical Naval Warfare System databases dealing with dynamic data, e.g., Readiness and Track vice Functional Database Manager provided reference data.

E-mail An electronic means for communication in which (a) usually text is transmitted, (b) operations include sending, storing, processing, and receiving information, (c) users are allowed to communicate under specified conditions, and (d) messages are held in storage until called for by the addressee.

Enterprise When used generically, an enterprise is defined as the aggregate of all functional elements participating in a business process improvement action regardless of the organizational structure housing those functional elements. (Note the difference in this definition and that of ENTERPRISE LEVEL. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Enterprise Level The Enterprise Level of the CIM Integration Architecture provides the geographic, technological, and managerial platform upon which all information systems development activity is based; it is the foundation that must support all that is built above it in the higher levels. In general, in this document it is synonymous with the entire Department of Defense. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Entity An element from the set of real-world objects (people, places, things, events, ideas) with characteristics in common and within the scope of the model. Each entity has a name that is a singular noun or noun phrase describing the object it represents. An entity is represented by a box. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, electronic Version)

Functional Integration Integration within the DoD of related and/or redundant business processes, in order to simplify, improve, and economize those processes. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Functional Process Improvement (also called **Business Process Re-engineering**) Application of a structured methodology to define a function's objectives and a strategy for achieving those objectives; its "as-is" and "to-be" process and data environments; its current and future mission needs and end-user requirements; and a program of incremental and evolutionary improvements to processes, data and supporting migration systems that are implemented through functional, technical, and economic analysis and decision making.

Procedures for conducting process improvement reviews and assessments in the DoD are provided in OASD (C4ISR) memoranda on Interim Management Guidance on Functional Process Improvement (August 5, 1992, and January 15, 1993). (DEPSECDEF Memo of 13 Oct. 1993, "Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement)

Guidance Any statement of direction or recommendation, not necessarily mandatory.

Help Desk The front line interface to the users to resolve any issue associated with information infrastructure-provided services.

IDEF Modeling Techniques A combination of graphic and narrative symbols and rules designed to capture the processes and structure of information in an organization. IDEF0 (pronounced IDEF-*zero*) is an activity, or behavior, modeling technique; IDEF1X (pronounced IDEF-*one-X*) is a rule, or data, modeling technique. IDEF modeling techniques were derived from the Integrated Computer Aided Manufacturing (ICAM) program sponsored by the U.S. Air Force. The acronym IDEF (pronounced *eye-deaf*) was formed from the term CAM **Def**inition Languages. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Individual Message. DMS Term. Individual Messaging. Includes working communications between individual DoD personnel with in administrative channels, both internal and external to the specific organizational element, including non-DoD users. Such messages do not generally commit or direct and organization. Individual messages do not require the same level of system management, priority/precedence, or assurance (signature/encryption) as organizational messages.

Information Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized databases, paper, microforms, or magnetic tape. (DoDD 8000.1 of 27 October 1992 (NOTAL))

Information Architecture A database schema of information categories (data sets) containing standardized data elements with designated data sources. The information architecture in the NWTDB Standards Manual is a guide for defining essential elements of information to support operational functionality, and for internal system design to achieve a common relational database. The NWTDB structure is hardware and software independent.

Information Distribution The ability to move information to all of the intended recipients.

Information Engineering The translation of certain types of process requirements into software programs. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Information Management The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructures. [DODD 8000.1]

The treatment of information as an asset to enhance an organization's competitiveness and responsiveness. It results from effectively identifying, collecting, and analyzing information — and then directing it to the points of decision making and customer service.

Information Protection (Same as Information System Security. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information Security The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

Information System Security The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. [NIS]

Information Standards The standardization of data elements, database structure, message text formats (MTFs), and tactical digital information links (TADILs).

Information System A system, whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information. (188) 2. Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. [NIS]

Information System Domain An information infrastructure controlled or managed by a single organizational entity. It normally includes a network, set of clients, servers, multi-media equipment, associated peripherals and network components interconnected and bounded by interfaces to external networks or communication circuits.

Information Technology The technology included in hardware and software used for Government information, regardless of the technology involved, whether computers, communications, micro-graphics, or others. [OMB Circular A-130 and DODD 8000.1.]

Information Technology Outreach Center An extension of the Information Technology Service Center (ITSC) where physical presence is required. Provides primarily hardware-related services such as device and cable plant maintenance, component replacement, software distribution and dial-in service. Act as the base “store front” for the ITSC.

Information Technology Service Center A center that provides comprehensive IM/IT support to a designated zone of the DON IT infrastructure. This includes information system operation, implementation support, and administration for a community of information producers and consumers. The ITSCs would be “Local Control Centers” in full compliance with the Joint Defense Information Infrastructure (DII) Control Centers (CC) Concept of Operations (CONOPS)

Each ITSC would perform three major duties:

- Integrated information system implementation, control and maintenance.
- Interface information flow from network to network including dial-in service.
- Consolidated information/application repository and distribution center for individual commands in the region.

Information Technology Standards Guidance A guiding information center that identifies the standards and provides the guidance for applying information technology toward the creation and sustainment of a responsive, and user-friendly, information management environment.

Information Transfer The process of moving messages containing user information from a source to a destination (sink). (188) Note: The information transfer rate may or may not be equal to the transmission modulation rate.

Integration Explicit top management initiatives to ensure that interdependent functions or systems operate efficiently for the overall benefit of the enterprise(i.e., the DoD). This contrasts with coordination among functions or systems, which ensures non-interference, but does not provide integration.

"Integration" implies seamless, transparent operation based on a shared or commonly-derived architecture (functional or technical) and standard data. "Interoperability" implies only the ability of a function or system to exchange information or services with another, separate function or system using translators or interchange rules/standards. (DEPSECDEF Memo of 13 Oct. 1993, "Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement)

Interface A boundary or point common to two or more command and control systems or subsystems, communication systems or equipment, or other entities across which necessary information flow takes place. A joint interface implies that the boundary is shared by two or more services/agencies. A combined interface is shared by entities from one or more U.S. services/ agencies and an allied nation.

(1) **Technical Interface**. A specification of the functional, electrical, and physical characteristics necessary to allow the exchange of information between systems. An Interface Requirements Specification (IRS) is used to specify the functional and physical requirements of an interface between systems; DI-MCCR-80026A pertains. An Interface Design Document (IDD) is used to describe the detailed design of the requirements within the IRS; DI-MCCR-80027A pertains. Warfare System Controlled Interface Documents (WSCIDs) are used to describe functional, physical, and electrical interface characteristics.

(2) **Procedural Interface**. A specification for accomplishing exchange of information across an interface; e.g., OPSPEC 411, OPSPEC 516, OPSPEC OTG. A procedural interface defines:

(a) The form or format in which information is to be exchanged.

(b) The prescribed information exchange language, syntax, and vocabulary to be used in the information exchange.

(c) The operating procedures that govern information exchange.

Infrastructure Infrastructure is used with different contextual meanings. Infrastructure most generally relates to and has a hardware orientation but note that it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. Again note that just citing standards for designing an architecture or infrastructure does not include functional and mission area requirements for performance. Performance requirement metrics must be an inherent part of an overall infrastructure to provide performance interoperability and compatibility. It identifies the top-level design of communications, processing, and operating system software. It describes the performance characteristics needed to meet database and application requirements. It provides a geographic distribution of components to locations. The infrastructure architecture is defined by the service provider for these capabilities. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs. [DOD 8020.1-M]

Intelligence The faculty or ability for comprehending and reasoning with facts, truths, or propositions; intellectual power; knowledge imparted or acquired; the collection of information; information communicated as news or notices. [Webster's]

Interoperability The ability of systems, units or forces to provide services to, and accept services from, other systems, units or forces, and to use the services so exchanged to enable them to operate effectively together (JCS Pub 1).

JINTACCS **Joint Interoperability of Tactical Command and Control Systems.** The JCS program encompassing approved standards for machine readable bit-oriented TADIL and man/machine readable character oriented MTF messages. (Replaced by USMTF.)

Key One or more attributes that may be used to uniquely identify an instance of an entity (as represented by a row in a database table). There are three types of keys:

Primary Key: The key chosen as the unique identifier for an entity. This key is migrated through the relationship to become the foreign key in child entities.

Alternate Key: A key that could also be used as a unique identifier for an entity, but is not selected for that purpose. For example, the entity EMPLOYEE could be uniquely identified by either SOCIAL-SECURITY-NUMBER or EMPLOYEE-ID-NUMBER. If EMPLOYEE-ID-NUMBER would be designated as the primary key, SOCIAL-SECURITY-NUMBER would be designated as an alternate key. Alternate keys are designated in the model by the notation (AK).

Foreign Key: A key in a child entity that is inherited from its parent entity. Only primary keys may migrate (be inherited). The foreign key may or may not become part of the primary key of the child. Each foreign key is designated by the notation (FK). (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version).

Knowledge Acquaintance with facts, truths, or principles, as from study or investigation; familiarity or conversance, as with a subject, language, or branch of learning; acquaintance with a thing, place, person, as by sight, experience, or report; the fact or state of knowing; perception of fact or truth; clear and certain mental apprehension; the state of being cognizant or aware. [Webster's]

Latency The length of the time interval between an event or stimulus and a response. In the context of IT latency refers to the amount of time it takes from the initiation of a control to the response of a control; or from an information query to the return of information.

Local Control Center A DII Control Center that manages CINC, Service, or Agency-unique networks, systems, applications, either deployed or fixed at a base, post, camp, or station. Supports community-of-interest or local assets regardless of its size or geographic dispersion. (JDIICC CONOPS)

Message Text Format(MTF) An approved standardized communication method using man/machine readable messages. MTF is characterized by its standardized, character-oriented message formats and transmission characteristics. United States Message Text Formats (USMTF) are JCS approved and mandated for both joint and intra-service usage. U.S. Navy tactical warfare systems also implement Navy-unique MTFs; e.g., OTH-T GOLD.

Migration System An existing automated information system (AIS), or a planned and approved AIS, that has been officially designated as the single AIS to support standard processes for a function. Other AISs, called “legacy systems, “that duplicate the support services provided by the migration system are terminated, so that all future AIS development and modernization can be applied to the migration system. A migration system is designated (or selected) by the OSD Principal Staff Assistant(s) and their Defense Component counterparts whose function(s) the system supports, with the coordination of the DoD Senior Information Management Official.

Upon selection and deployment, the migration system becomes the single AIS baseline for:

• Incremental and evolutionary changes that are required to implement functional process improvements, or to execute additional responsibilities assigned to the function that the system supports.

• Technical enhancements that implement standard data and integrated databases, and that migrate the system toward an open systems environment and a standards-based architecture defined by the DoD Technical Architecture Framework for Information Management.

(DEPSECDEF Memo of 13 Oct 1993, “Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement)

Mission A primary task, vision, or purpose of an organization or operation.

Mission Application An application that supports a particular mission. In the ITSG context it means special support to uniquely military requirements. Analogous to “Operational Application”.

Model A representation of a complex, real-world phenomenon such that it can answer questions about the real-world phenomenon within some acceptable and predictable tolerance. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

National Information Infrastructure A proposed, advanced, seamless web of public and private communications networks, interactive services, interoperable hardware and software, computers, databases, and consumer electronics to put vast amounts of information at users' fingertips. Note: NII includes more than just the physical facilities (more than the cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave nets, switches, televisions, monitors, and printers) used to transmit, store, process, and display voice, data, and images; it encompasses a wide range of interactive functions, user-tailored services, and multimedia databases that are interconnected in a technology-neutral manner that will favor no one industry over any other. Synonym: "Information Superhighway". [FS 1037C]

Naval Warfare Tactical Database (NWTDB) (1) The management process to evolve to the common tactical database that supports Naval, Joint, and Combined operations.

(2) The authoritative tactical database, or subsets thereof, distributed by designated producers in accordance with the information architecture contained in the functional volumes which comprise the NWTDB Standards Manual.

Network The set of switching and transmission subsystem communication components to support information transfer. The network includes all hardware and software communication components residing in switching, routing, and transmission subsystem components, as well as communication-related hardware and software and those components that reside in hosts (e.g., communication protocols). The network also includes the organization and configuration of embedded hardware and software to support orderly and logical information distribution.

Network Centric A systems engineering concept where end systems are attached to a shared network rather than directly to each other.

Network Centric Warfare A warfighting and deterrence concept that takes advantage of a shared network to exchange information and provide direction thereby increasing speed of command and reducing observe-orient-decide-act (OODA) cycle.

Network centric warfare includes network centric systems engineering concepts but also several other components such as force structure and doctrine. Only the network centric systems engineering concept is within the scope of the ITSG.

Network Information Center The Network Information Center (NIC) registers hosts and domains, assigns IP network numbers and Autonomous System Numbers for network entities, and provides domain name system server files to the network community.

Network Management Center A central location for network management. If functions as a control center for network control monitoring, analysis and accounting. A management center can contain a Network Information Center as well as a Network Operating Center.

Network Monitoring Center A central location for network management. If functions as a control center for network monitoring, analysis and accounting.

Network Operations Center A central location for network management. If functions as a control center for network control monitoring, analysis and accounting.

Node 1. In network topology, a terminal of any branch of a network or an interconnection common to two or more branches of a network. (188) Synonyms junction point, nodal point. 2. In a switched network, one of the switches forming the network backbone. Note: A node may also include patching and control facilities. (188) 3. A technical control facility (TCF). (188)

Normalization A set of tests that ensure stable groupings of ATTRIBUTES (by housing them in the appropriate ENTITIES) and their relationships. This “quality control test” against a FULLY-ATTRIBUTED RULE MODEL eliminates data redundancy and allows it to be readily extensible as new data are discovered. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Open System One that consists of modular, multi-vendor interoperable building blocks that are assembled into functional units.

Operational Applications An application that supports a particular operation or mission. Normally military unique. Analogous to “Mission Application”.

Operational Environment The physical condition which surrounds or contains a military platform while conducting operations.

Operational Specification(OPSPEC) A U.S. Navy specification for a Navy procedural interface.

Organizational Message Message for command correspondence within DMS. Organizational Messaging. Includes messages and other communications exchanged between organizational elements in support of command and control, combat support, combat service support, and other functional activities. Typically these messages provide formal direction, establish a formal position, commitment, or response for the organization. Organizational messages require approval for transmission by designated officials of the sending organization and determination of internal distribution by the receiving organization. Because of their official and sometimes critical nature, such messages impose operational requirements on the communications systems for capabilities such as precedence, timely delivery, and high availability and reliability. Organizational messages must be signed in order to provide proof of participation and audit/trace capability.

OTH-T GOLD (OTG) Over-the-Horizon Targeting GOLD, a CNO approved man/ machine readable character oriented message standard for information exchange between tactical systems.

Peripheral (Peripheral Equipment): In a data processing system, any equipment, distinct from the central processing unit, that may provide the system with additional capabilities. Note: Such equipment is often offline until needed for a specific purpose and may, in some cases, be shared among several users. [FS 1037C]

Policy A standing set of general principles or guidelines on a topic deemed to be mandatory.

Practice A way of doing something.

Product A service or the end result of a service which can be a change in state, a physical item, a desired tool or stimulus.

Recommendation Guidance, not mandatory, that if followed should produce the desired result.

Reference Data Data used to amplify or clarify a tactical data set. e.g., organizational names or airframe dimensions.

Requirement Something that is needed, normally to complete or enhance mission capability

Risk Exposure to the chance of an adverse occurrence.

Risk Avoidance Minimizing the exposure to adverse occurrences.

Risk Management The act of balancing risk that is inherent in the operational environment with activities that must occur to accomplish a mission. The exposure to adversity normally conflicts with the need to complete a mission, particularly in the military context.

Recommendation Guidance provided to assist one in performing a task or completing a mission.

Rule Model The result of applying the rule modeling technique. It is a graphic or structured narrative representation of the data meanings and business rules in an organization. The model is represented in IDEF1X by a set of graphic diagrams that represent classes of real or abstract objects, their attributes, and their relationships to one another. Rule model diagrams are refined with three different levels of detail: The ENTITY-RELATIONSHIP LEVEL, the KEY-BASED LEVEL, and the FULLYATTRIBUTED LEVEL. The model includes a GLOSSARY and BUSINESS STATEMENTS or rules.

Rule Model Levels There are three levels of rule model refinement: Entity-Relationship, Key-Based, and Fully Attributed.

Entity-Relationship Model: This diagram is the least refined. It shows entities and their relationships. The relationships at this level may be nonspecific. You may add attributes at this level if they are known, but it is not required to do so.

Key-Based Model: This diagram starts with the E-R diagram and eliminates any nonspecific relationships by adding an associative or intersection entity. Keys are added to the entities and migrated. You may add any known non-key attributes at this level, but it is not required to do so.

Fully Attributed Model: This diagram starts with the key-based model and adds the non-key attributes. Several tests are applied to the model to ensure that it is in third normal form. (Corporate Information Management Process Improvement Methodology for DoD Functional Managers, 2d Edition, Electronic Version)

Server Computers, including workstations and mainframes, that provide information services to a network.

Service Desk The front line outreach center to minimize disruption to user operations during system upgrades and configurations changes. The Service Desk supports change control, coordination, approval, and implementation.

Specification A well defined, well described design, protocol, or practice.

A document prepared to support acquisition that describes the essential technical requirements for purchased material and the criteria for determining whether the requirements are met. [DOD 4120.3-M]

Standard A selected and approved specification or set of specifications by an authoritative body.

A document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. Standards may also establish requirements for selection, application, and design criteria of material. [DOD 4120.3-M]

System Architecture A set of interconnected elements constituted to achieve a given objective by performing specified functions. (IEEE Dictionary)

Tactical Data Data used in direct support of tactical decision making or in support system functions that provide options or recommendations to decision makers. Examples include speed of platforms, operating parameters of systems, enemy capabilities, etc.

Tactical Digital Information Link (TADIL) A JCS approved standardized communications link suitable for transmission of machine only readable information. A TADIL is characterized by its standardized, bit-oriented message formats and transmission characteristics.

Tactical Information Interoperability The ability of tactical Naval warfare systems to use approved joint and Navy information standards, especially Joint Interoperability of Tactical Command and Control Systems (JINTACCS), Naval Warfare Tactical Database (NWTDB), and/or OTH-T GOLD formats.

Tactical Naval Warfare System Any C4ISR or combat system that supports Naval warfare.

Time-Late The time difference between time of the discovery or data creation, and the present time.

Teleconference The live exchange of information among persons and machines remote from one another but linked by a telecommunications system. Note: The telecommunications system may support the teleconference by providing audio, video, and data services by one or more means, such as telephone, telegraph, teletype, radio, and television. (188)

Understanding The ability or power to acquire and interpret knowledge; comprehension; intelligence; mental faculties or power of discernment; personal interpretation; knowledge of a particular field; ability to cope or deal with something;

USMTF United States Message Text Format An approved standardized communication method using man/machine readable messages. MTF is characterized by its standardized, character-oriented message formats and transmission characteristics.

Wisdom The faculty to discern right and truth and to judge or act accordingly; sound judgment, sagacity, discretion, common sense, extensive knowledge. [Webster's]

Appendix C - Selected Guidance Justification

This appendix provides the supporting rationale for not selecting or using the IT products that are listed in the ITSG as “Not Recommended.” It also provides rationale for choosing a particular product or limiting standard – referred to in this Appendix as “Preferred Product.”

The specific guidance used in selecting standards (and products) is that they should meet the following criteria: (1) security, (2) interoperability, (3) functionality, (4) performance, and (5) business factors such as cost and market availability. Products are either “Not Recommended” or selected as “Preferred Products” based on this criteria.

Security. Information protection involves both system security and information security. Selected standards must support the ability to provide both system and information security.

Functionality. Standards and guidance must support the fundamental requirement to ensure that IM/IT systems effectively and efficiently support the operational mission/requirements.

Interoperability. Applications and computers from different suppliers will have the capability to work together on a network and to connect and share data and processes as appropriate. The model that the standards in this document follow is one that allows end systems to attach to any point on an internetwork. (End systems include clients, servers, and sensors that produce or consume information.)

Performance. The degree of quality that a particular standard or guidance provides in selecting IM/IT products or services.

Business. Implementation cost and market acceptance of the standard or guidance is also a selection factor. Market acceptance is judged more on market momentum than on current market share. A dominant product may actually be losing market share, while an emerging product or standard may be rapidly increasing its share. By including market acceptance as one of the selection criteria, we obtain a balance in theoretical versus practical value as based on the market conclusions regarding technology, functionality and value.

Chapter 3: Information Protection

Table 3-2: Zone 4 VPN Implementations

Not Recommended:	Proprietary VPN products			
Security	Functionality	Interoperability	Performance	Business
●		●		

Rationale: Limited interoperability, multi-vendor interoperability is a problem. It is generally more difficult to assess the security properties of proprietary products because the details of their interfaces, design, and operation are known only to the vendor. To assess the security properties requires a potentially expensive and lengthy evaluation.

Table 3-7: Operating System Security

Not Recommended:	Windows 3.1			
Security	Functionality	Interoperability	Performance	Business
●	●	●		

Rationale: No NSA C2 security features. Does not adequately perform identification, authentication, and access control in multi-user/networked environment. Systems that are primarily single user with limited networking capability may consider non-C2 OSs when C2 alternatives are not adequate, e.g., laptops. Limited interoperability, no built in TCP/IP protocol suite.

Preferred Product:	Windows NT			
Security	Functionality	Interoperability	Performance	Business
	■	■	■	■

Rationale: Product of choice in approximately 99 percent of DON PCs and 78 percent of world PCs. Provides satisfactory interoperability, functionality and performance. Provides strong justification for supportability/business because of commonality.

Not Recommended:	MS-DOS			
Security	Functionality	Interoperability	Performance	Business
●	●	●		

Rationale: No NSA C2 security features. Does not adequately perform identification, authentication, and access control in multi-user/networked environment. Systems that are primarily single user with limited networking may consider non-C2 OSs when C2 alternatives are not adequate, e.g., laptops. Limited interoperability, no built in TCP/IP protocol suite.

Table 3-8: Data at Rest Encryption

Not Recommended:	Products with proprietary algorithms			
Security	Functionality	Interoperability	Performance	Business
●			●	

Rationale: Administration difficulty in instances of transferred personnel or casualties. It is generally more difficult to assess the security properties of proprietary products due to the fact that the details of their interfaces, design, and operation are known only to the vendor. To assess the security properties requires a potentially expensive and lengthy evaluation.

Chapter 4: Facility and Environmental Requirements

None

Chapter 5: Information Transfer

Table 5.2: Personal Workstation Operating Systems

Not Recommended:	ARCnet			
Security	Functionality	Interoperability	Performance	Business
	●	●	●	●

Rationale: Not routable, item cannot span routers and edge devices well, and is limited to a physical LAN. Not scalable, the item solves a niche market. Limited interoperability, the item

may solve a short term problem but will lead to interoperability problems. Low performance, the item has limited performance characteristics, and may not work in certain areas. Not commercially viable, the item is old, no longer supported and viewed as out-dated by industry practice. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	100VG AnyLAN			
Security	Functionality	Interoperability	Performance	Business
	●	●		●

Rationale: Not scalable, the item solves a niche market. Limited interoperability, the item may solve a short term problem but will lead to interoperability problems. Not commercially viable, the item is old, no longer supported and viewed as out-dated by industry practice. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	Token Ring			
Security	Functionality	Interoperability	Performance	Business
	●		●	●

Rationale: Not scalable, the item solves a niche market (which would lead to a lack of interoperability). Low performance, the item has limited performance characteristics, and may not work in certain areas. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	AppleTalk			
Security	Functionality	Interoperability	Performance	Business
	●	●	●	●

Rationale: Not routable with Open Shortest Path First/Border Gateway Protocol (OSPF/BGP). Not scalable, the item solves a niche market. Low performance, the item has limited performance characteristics, and may not work in certain areas. Limited interoperability, the item may solve a short term problem but will lead to interoperability problems. Not commercially viable, the item is old, no longer supported and viewed as out-dated by industry practice. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	SNA/APPN			
Security	Functionality	Interoperability	Performance	Business
	●	●		●

Rationale: Not routable with Open Shortest Path First/Border Gateway Protocol (OSPF/BGP). Limited interoperability, the item may solve a short term problem but will lead to interoperability problems. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	Novell IPX			
Security	Functionality	Interoperability	Performance	Business
	●	●		●

Rationale: Not routable with Open Shortest Path First/Border Gateway Protocol (OSPF/BGP). Not scalable, the item solves a niche market. Limited interoperability, the item may solve a short term problem but will lead to interoperability problems. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	NetBEUI			
Security	Functionality	Interoperability	Performance	Business
	●	●		●

Rationale: Not routable with Open Shortest Path First/Border Gateway Protocol (OSPF/BGP). Not scalable, the item solves a niche market. Limited interoperability, the item may solve a specific problem but create interoperability problems. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	Banyan VINES			
Security	Functionality	Interoperability	Performance	Business
	●	●		●

Rationale: Interoperability, VINES version of IP requires special interfaces to make interoperable with IAB Internet Protocol; may not work in other IP environments. Limited market acceptance, and long term supportability make cost of ownership unattractive.

Not Recommended:	DecNET/LAT			
Security	Functionality	Interoperability	Performance	Business
	●	●		●

Rationale: Not routable with Open Shortest Path First/Border Gateway Protocol (OSPF/BGP). Not scalable, the item solves a niche market. Limited interoperability, the item may solve a specific problem but will lead to interoperability problems. Not commercially viable, the item is old, no longer supported and viewed as out-dated by industry practice. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	OpenAir 2.4 Wireless			
Security	Functionality	Interoperability	Performance	Business
●	●	●		●

Rationale: This product is not IEEE 802.11 compliant but based upon a proprietary specification. This presents open system and long term supportability problems.

Not Recommended:	ETS 300 653			
Security	Functionality	Interoperability	Performance	Business
	●	●	●	

Rationale: This product is not IEEE 802.11 compliant but based upon European specification that results in inadequate frequency band availability due to FCC restrictions. This product will be reevaluated when this is resolved.

Not Recommended:	HIPERLAN Wireless			
Security	Functionality	Interoperability	Performance	Business
	●	●	●	

Rationale: This product is not IEEE 802.11 compliant but based upon European specification that results in inadequate frequency band availability due to FCC restrictions. This product will be reevaluated when this is resolved.

Table 5.3: Physical and Data Link for WANs

Not Recommended:	Commercial Internet Service Providers			
Security	Functionality	Interoperability	Performance	Business
●				

Rationale: Not secure, lack of control by DoD, limited Virtual Private Network support. DON IT architecture will keep this functionality in-house.

Not Recommended:	OpenAir2.4 Wireless			
Security	Functionality	Interoperability	Performance	Business
●	●	●		●

Rationale: This product is not IEEE 802.11 compliant but based upon a proprietary specification. This presents open system and long term supportability problems.

Table 5-6: Network and Transport Layer

Not Recommended:	Novell IPX			
Security	Functionality	Interoperability	Performance	Business
	●	●	●	●

Rationale: Not scalable, the item solves a niche market. Limited interoperability, the item may meet a short term requirement but will lead to interoperability problems. Because of DON dependence on radio WANs and their limited bandwidth, operational requirements necessitate limiting the number of routing protocols. Not routable with Open Shortest Path First/Border Gateway Protocol (OSPF/BGP). (We have chosen OSPF/BGP as the sole gateway protocol based on JTA; protocol suites that cannot operate within that routing information framework should be avoided.) Limited mission market acceptance, the item may be widespread in certain markets but not in the mission areas that the DON needs to work in.

Not Recommended:	Banyan VINES			
Security	Functionality	Interoperability	Performance	Business
	●	●	●	●

Rationale: Interoperability, VINES version of IP requires special interfaces to make interoperable with IAB Internet Protocol; may not work in other IP environments. Limited market acceptance, and long term supportability make cost of ownership unattractive. Because of DON dependence on radio WANs and their limited bandwidth, operational requirements necessitate limiting the number of routing protocols. Not routable with Open Shortest Path First/Border Gateway Protocol (OSPF/BGP). (We have chosen OSPF/BGF as the sole gateway protocol based on JTA; protocol suites that cannot operate within that routing information framework should be avoided.)

Table 5-7: Network Routing Protocols

Not Recommended:	IPNetBEUI			
Security	Functionality	Interoperability	Performance	Business
	●			●

Rationale: Not routable with Open Shortest Path First/Border Gateway Protocol (OSPF/BGP). Not scalable, the item solves a niche market (which would lead to a lack of interoperability). Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	LAT			
Security	Functionality	Interoperability	Performance	Business
	●	●		●

Rationale: Not routable, item cannot span routers and edge devices well, and is limited to a physical LAN. Not scalable, the item solves a niche market. Limited interoperability, the item may solve a short term problem but will lead to interoperability problems. Not commercially viable, the item is old, no longer supported and viewed as out-dated by industry practice. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	IGRP			
Security	Functionality	Interoperability	Performance	Business
	●			●

Rationale: Vendor proprietary protocol, we have chosen Open Shortest Path First/Border Gateway Protocol (OSPF/BGP) instead. Not scalable, the item solves a niche market (which would lead to a lack of interoperability) and is not a scalable solution. Not commercially viable, the item is old, no longer supported and viewed as out-dated by industry practice. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas.

Not Recommended:	RIP			
Security	Functionality	Interoperability	Performance	Business
●	●		●	●

Rationale: Routing Information Protocol (RIP) is not a scalable solution. Version 1 lacks authentication and version 2 is not as efficient as OSPF. Affordability is major issue.

Chapter 6: Information Distribution

Table 6-11: Web Client

Preferred Product:	Java			
Security	Functionality	Interoperability	Performance	Business
■	■	■	■	■

Rationale: Provides server level protection not afforded by Active X. Provides open systems basis for interoperable application solutions. Functionality of Java products is revolutionizing

information management. Market acceptance provides widespread use in markets that the DON needs to work in.

Chapter 7: Computing Resource

Table 7-12: Personal Workstation Operating Systems

Not Recommended:	MS Windows 3.1 and older			
Security	Functionality	Interoperability	Performance	Business
●	●			●

Rationale: No TCP/IP except through third parties. Does not have NSA C2 certification. Replaced by more robust product. Not commercially viable, the item is old, no longer supported and viewed as out-dated by industry practice. No NSA C2 security features.

Not Recommended:	OS/2			
Security	Functionality	Interoperability	Performance	Business
●				●

Rationale: Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas. Supportability, increasing the number of DON products supported proportionally increases cost of ownership. No NSA C2 security features.

Not Recommended:	MacOS			
Security	Functionality	Interoperability	Performance	Business
●	●			●

Rationale: Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas. Supportability, increasing the number of products supported proportionally increases cost of ownership. Not functional on the desktop PC in use by majority of DON organizations. No NSA C2 security features.

Preferred Product:	Windows NT			
Security	Functionality	Interoperability	Performance	Business
●	●	●	●	●

Rationale: Both NT and UNIX are DoD COE compliant; NT and some UNIX are NSA C2 certified; only NT is DMS compliant; therefore, DON has selected NT as the preferred product. DON has determined to have a single homogeneous client for supportability, and reduced life cycle costs. Supports interoperability both in Navy and Marine Corps because of numbers purchased in last 18 months vis-à-vis all other OS products, and likewise reduces supportability costs because of reduced numbers of products

Preferred Product:	Windows 95			
Security	Functionality	Interoperability	Performance	Business
		●		●

Rationale: Supports interoperability both in Navy and Marine Corps and across DoD because of consumer acceptance based on numbers of items being purchased in last 12 months vis-a-vis all other OS products. Economically viable because of reduced life cycle cost associated with system support.

Table 7-13: Server Operating Systems

Not Recommended:	NetWare 3.x or less			
Security	Functionality	Interoperability	Performance	Business
	●	●		

Rationale: Limited interoperability, no built in TCP/IP protocol suite, replaced by new version. Limited mission market acceptance, the item may be widespread in certain markets but not in the DON mission areas. Supportability, increasing the number of products supported proportionally increases cost of ownership.

Not Recommended:	Banyan VINES			
Security	Functionality	Interoperability	Performance	Business
	●			●

Rationale: Limited interoperability, no built in TCP/IP protocol suite. Supportability, increasing the number of products supported proportionally increases cost of ownership.

Chapter 8: Information Management

None

Chapter 9: Applications

None

Chapter 10: Enterprise Management

None

Appendix D - Supporting IT Contracts

Selected products (preferred products) have appeared in the ITSG "Recommended Implementation" timelines and are also addressed in Appendix C – Selected Guidance Justification (along with the "Not Recommended" products). Appendix D – Supporting IT Contracts, contains a list of available, competitively awarded contracts by which these preferred products can be obtained. Additional information and updates to this appendix may be obtained from the Information Technology Electronic Commerce (ITEC) Direct link under the DON CIO web page http://www.itec-direct.navy.mil.

This appendix is arranged by contract vehicle, point of contact (where available), contract line item, and description. Where links are available directly to the vehicle, they are provided.

Summary of Contents:

- TAC Joint Workstations
- TAC Notebook
- TAC PC
- PC-LAN+
- SUPERMINI
- DBM
- CAD-2 NAVFAC (IM/FCAD2)
- CAD-2 NAVAIR/SPAWAR
- CAD-2 NAVSEA
- NTOPS
- FISC Philadelphia
- ViViD

TAC Joint Workstations
Vehicle: N68939-97-A-0013
Silicon Graphics
POC: Doug Romig (619) 553-4086
CLIN/BLIN: AC-SW013

Description: Cosmo Code Java Development Environment for 5.3, 6.2, and 6.3 node-lock single user. The Cosmo Code development environment provides tools to create Java applets, applications and packages interactively, compile and manage projects, and debug and browse programs.

TAC Notebook
Vehicle: N68939-96-A-0002
McBride
POC: Doug Romig (619) 553-4086
http://itec-direct.navy.mil/mcb-nb.html
CLIN/BLIN: U1303
Description: Site License Fee for Windows 95 Endpoint (Part # OGM-W95)

CLIN/BLIN: U1304
Description: One-time software upgrade fee for out-of-support customers running: Windows NT (Part # OGM-WNT-SWF)

CLIN/BLIN: U1190
Description: Site License Fee for Windows NT Endpoint (Part # OGM-WNT)

TAC PC
Vehicle: N68939-96-A-0006
GTSI
POC: Doug Romig (619) 553-4086
CLIN/BLIN: 3493-123424
Description: Windows 95 Version Upgrade. Windows 95 Version Upgrade from Windows 3.x and Windows for WorkGroups 3.0x. (Part # 050-050-95VL)

CLIN/BLIN: 3493-123538
Description: Windows NT Client Access. Windows NT Client Access 4.0 – English; License (Part # 2272075V40VL)

CLIN/BLIN: 3493-123541
Description: Windows NT Server. Windows NT Server 4.0 – English; License (Part # 2273275V40VL)

CLIN/BLIN: 3493-123533
Description: Windows NT Workstation. Windows NT Workstation 4.0 – English; Upgrade from Windows NT 3.x (Part # 236-274-40VL)

PC-LAN+
Vehicle: N68939-95-D-0018
EDS
POC: Christa LeBoeuf (619) 524-7599
http://www.eds-ms.com/pclhome.htm

Note: The Contractor provides a one-year warranty for all software provided under this contract. During the warranty period, all updates, upgrades, and new releases (accepted by the Contracting Officer) shall be provided at no additional charge.

CLIN/BLIN: 1000AA
Description: MS Windows NT Server 4.0 100 User License

- Media-CD-ROM.
- Includes TCP/IP services, NetWare services, OS/2 services, Macintosh services, and Remote Access service,
- Bundled with Windows NT Resource Kit
- NT Clients: 100 users in an combo of NetBIOS, RAS, RCP/IP, Windows (NetBIOS, TCP/IP,IPX), WFW (NetBIOS, TCP/IP,IPX), DOS (NetBIOS, TCP/IP,IPX), Novell Client (IPX, TCP/IP), Pathworks Client (NetBIOS), LAN Manager, LAN Manager OS/2, Banyan (Vines and NetBIOS) Note for 1000AA/1000AB: The Client Redirector Software, LAN Manager for MS-DOS v2.2c and Network Client v3.0 for MS-DOS are provided free on CD-ROM. Also provided on CD-ROM is Windows for Workgroup 3.11 code only (purchase license under SCLIN 1130AA).

CLIN/BLIN: 1000BA
Description: MS Windows NT Server 4.0 50 User License

- Media - CD-ROM
- Includes TCP/IP services, NetWare services, OS/2 services, Macintosh services, and Remote Access service,
- Bundled with Windows NT Resource Kit
- NT Clients: 50 users in an combo of NetBIOS, RAS, RCP/IP, Windows (NetBIOS, TCP/IP,IPX), WFW (NetBIOS, TCP/IP,IPX), DOS (NetBIOS, TCP/IP,IPX), Novell Client (IPX, TCP/IP), Pathworks Client (NetBIOS), LAN Manager, Lan Manager OS/2, Banyan (Vines and NetBIOS) Note for 1000AA/1000AB: The Client Redirector Software, LAN Manager for MS-DOS v2.2c and Network Client v3.0 for MS-DOS are provided free on CD-ROM. Also provided on CD-ROM is Windows for Workgroup 3.11 code only (purchase license under SCLIN 1130AA).

CLIN/BLIN: 1000CA
Description: MS Windows NT Server 4.0 25 User License

- Media - CD-ROM
- Includes TCP/IP services, NetWare services, OS/2 services, Macintosh services, and Remote Access service,
- Bundled with Windows NT Resource Kit
- NT Clients: 25 users in an combo of NetBIOS, RAS, RCP/IP, Windows (NetBIOS, TCP/IP,IPX), WFW (NetBIOS, TCP/IP,IPX), DOS (NetBIOS, TCP/IP,IPX), Novell Client (IPX, TCP/IP), Pathworks Client (NetBIOS), LAN Manager, LAN Manager OS/2,

Banyan (Vines and NetBIOS) Note for 1000AA/1000AB: The Client Redirector Software, LAN Manager for MS-DOS v2.2c and Network Client v3.0 for MS-DOS are provided free on CD-ROM. Also provided on CD-ROM is Windows for Workgroup 3.11 code only (purchase license under SCLIN 1130AA).

CLIN/BLIN: 1000DA
Description: MS Windows NT Server 4.0 250 User

- Media - CD-ROM.
- Includes TCP/IP services, NetWare services, OS/2 services, Macintosh services, and Remote Access service,
- Bundled with Windows NT Resource Kit
- NT Clients: 250 users in an combo of NetBIOS, RAS, RCP/IP, Windows (NetBIOS, TCP/IP,IPX), WFW (NetBIOS, TCP/IP,IPX), DOS (NetBIOS, TCP/IP,IPX), Novell Client (IPX, TCP/IP), Pathworks Client (NetBIOS), LAN Manager, Lan Manager OS/2, Banyan (Vines and NetBIOS) Note for 1000AA/1000AB: The Client Redirector Software, LAN Manager for MS-DOS v2.2c and Network Client v3.0 for MS-DOS are provided free on CD-ROM. Also provided on CD-ROM is Windows for Workgroup 3.11 code only (purchase license under SCLIN 1130AA).

CLIN/BLIN: 1002AA
Description: MS Windows NT Workstation 4.0 – full pkg., Single User License. Includes one set of documentation, one CD-ROM, one set of Start Up Diskettes, and a single user license

CLIN/BLIN: 1002AB
Description: MS Windows NT Workstation 4.0 – full pkg., 100 Users License. Includes one set of documentation, one CD-ROM, one set of Start Up Diskettes, and 100 users license

CLIN/BLIN: 1002AC
Description: MS Windows NT Workstation 4.0 – full pkg., 50 Users License. Includes one set of documentation, one CD-ROM, one set of Start Up Diskettes, and 50 users license

CLIN/BLIN: 1002AD
Description: MS Windows NT Workstation 4.0 – full pkg., 25 Users License. Includes one set of documentation, one CD-ROM, one set of Start Up Diskettes, and 25 users license

CLIN/BLIN: 1002AE
Description: MS Windows NT Workstation 4.0 – full pkg., 1000 Users License. Includes one set of documentation, one CD-ROM, one set of Start Up Diskettes, and 1,000 users license

CLIN/BLIN: 1002AF
Description: MS Windows NT Workstation 4.0 – full pkg., 2500 Users License. Includes one set of documentation, one CD-ROM, one set of Start Up Diskettes, and 2,500 users license

CLIN/BLIN: 1002BA

Description: MS Windows NT Client Access 4.0, English, 1-50 users. Windows NT Client Access 4.0 - English, 1-50 users, license only, for clients that operate on NT Server network, use this price for each user

CLIN/BLIN: 1002BB
Description: MS Windows NT Client Access 4.0, English, 51-100 users Windows NT Client Access 4.0 - English, 51-100 users, license only, for clients that operate on NT Server network, use this price for each user

CLIN/BLIN: 1002BC
Description: MS Windows NT Client Access 4.0, English, 101-250 users. Windows NT Client Access 4.0 - English, 101-250 users, license only, for clients that operate on NT Server network, use this price for each user

CLIN/BLIN: 1002BD
Description: MS Windows NT Client Access 4.0, English, 251-500 users. Windows NT Client Access 4.0 - English, 251-500 users, license only, for clients that operate on NT Server network, use this price for each user

CLIN/BLIN: 1002BE
Description: MS Windows NT Client Access 4.0, English, 501-1000 users. Windows NT Client Access 4.0 - English, 501-1000 users, license only, for clients that operate on NT Server network, use this price for each user.

CLIN/BLIN: 1002BF
Description: MS Windows NT Client Access 4.0, English, 1001+ users. Windows NT Client Access 4.0 - English, 1000+ users, license only, for clients that operate on NT Server network, use this price for each user.

CLIN/BLIN: 1002BG
Description: MS Windows NT Client Access License Version Upgrade 4.0. Windows NT Client Access License Version Upgrade 4.0, no maintenance, use this price for each user, quantity one and above.

Java – Proposal under evaluation

JavaScript – Proposal under evaluation

SUPERMINI
Vehicle: F19630-93-D-0001
LITTON/PRC
POC: Lyn Purvis (619) 524-7541
http://eagle.is.prc.com/smp/index.htm
CLIN/BLIN: 1010AA
Description: MS Windows NT Server OS. An integrated server software and operating system for symmetrical, multiprocessor workstations. Requires a minimum of one CLIN 1010AB.

CLIN/BLIN: 1010AB
Description: MS Windows NT 16-User License. A 16-User license for client access of NT Server OS. Requires the purchase of CLIN 1010AA.

DBM
Vehicle: F19628-93-D-0018

TMA
POC: Brian Wolstencroft (619) 524-7539
CLIN/BLIN: 1007BF
Description: MS Windows NT Server V4.x Operating System with 5 Clients

Part # 227-00028

Price is for Unit Perpetual License Fee

CLIN/BLIN: 2007BF - Unit Monthly Maintenance

CLIN/BLIN: 1007BG
Description: MS Windows NT Server V4.x Operating System with 10 Server v4.x Client Licenses

Part # 227-00027

Price is for Unit Perpetual License Fee

CLIN/BLIN: 2007BG - Unit Monthly Maintenance

CLIN/BLIN: 1007BH
Description: MS Windows NT Server V4.x Client License for a single client. Part # 351-00187. Price is for Unit Perpetual License Fee. License for a single client to access any Windows NT Server in a network. These are required for any computer, including those running any computer, including those running Windows for Workgroups, Windows 95, or Windows NT Workstation. Acquired separately from Windows NT Server, Enterprise Edition.

CLIN/BLIN: 2007BH
Description: Unit Monthly Maintenance for CLIN 1007 BH.

CLIN/BLIN: 1007BJ
Description: MS Windows NT Server V4.x Client License for 50 clients. Part # 351-00220. Price is for Unit Perpetual License Fee.

CLIN/BLIN: 2007BJ - Unit Monthly Maintenance

CLIN/BLIN: 1007BK
Description: MS Windows NT Server V4.x Client License for 500 clients. Part # 351-00222. Price is for Unit Perpetual License Fee.

CLIN/BLIN: 2007BK - Unit Monthly Maintenance

CLIN/BLIN: 1007BL
Description: MS Windows NT Server V4.x Client License for 1000 clients. Part # 351-00224. Price is for Unit Perpetual License Fee.

CLIN/BLIN: 2007BL - Unit Monthly Maintenance

NOTE: There is no Software Warranty on the contract other than for those items that fail to pass the acceptance test within the prescribed acceptance test period. Software maintenance is available on the Contract and may be purchased. TMA includes software maintenance CLINs and

prices on all quotes for software. Failure to order software maintenance will preclude updates to the software.

CAD-2 NAVFAC (IM/FCAD2)
Vehicle: N66032-93-D-0021
Intergraph
POC: Tony Hinsen (703) 325-7360
http://cad2www.cordant.com/cad/navfac.htm
CLIN/BLIN: A013BG
Description: MS Windows NT Workstation SW (V4.0) one client license Microsoft Windows NT is the 32-bit, multithreaded, multitasking operating system for Intel-based workstations. SH**265 is Microsoft Windows NT Workstation version 4.0 with support for up to two processors. ADV level support includes phone support assistance with installation, configuration and trouble-shooting the use of:

NTW operating system,

Intergraph drivers (SCSI, video and network) and HAL,

Network protocols (NetBEUI, TCP/IP, DLC, NWLink IPX/SPX, and DHCP, and connectivity,

Services: Netware client, RAS, WINS, and DHCP,

Printer/peripheral drivers for devices purchased from Intergraph. Also error message interpretation for NTW and drivers. NTW "bug" reporting to Microsoft. Driver bug reporting to Intergraph with fixes provided via IBBS/ftp/www site. Version upgrades are available from SHK0265. Note: Installation is not included. Installation of the software may be performed by qualified Government personnel or installation services may be purchased separately from the Intergraph CAD-2 contract.

CLIN Part Number(s):

- SHBY265AA-0400A - Microsoft NT Workstation S/W for CAD-2
- SHK0265A3-0100E - Microsoft NT Workstation S/W For CAD-2

Monthly Maintenance - A013BGS Software Support

CAD-2 NAVFAC (IM/FCAD2)
Vehicle: N66032-93-D-0022
TRACOR
POC: Tony Hinsen (703) 325-7360
CLIN/BLIN: C040AX
Description: MS Windows NT Server Operating System. Microsoft NT Server is a multi-purpose network operating system that offers file and print services while providing the infrastructure to run client-server applications. Windows NT server also integrates a broad range of communications services and tools for handling network management ranging from small workgroups to an enterprise network. *Multiple User Perpetual License (MUPL); Perpetual Right-to-Use License.

CLIN/BLIN: C040BE

Description: MS Windows NT Workstation Operating Software. Microsoft Windows NT Workstation provides the end-user with the foundation to work in a multi-processing environment. Using the capabilities of a 32-bit multi-tasking operating system and symmetric multiple processing (SMP) support, Windows NT Workstation can handle more resource intensive tasks. In addition, it is configurable to integrate into existing networks with built-in driver support for TCP/IP and IPX/SPX protocols.

CLIN/BLIN: C040CN
Description: Windows NT Server Client Access. Part No: NT SRVR CAL. Microsoft NT Server Client Access allows additional clients access to an existing server hosting Microsoft NT Server. For servers hosting a large number of workstations, it is crucial to have the flexibility to increase the number of users as needed in increments of one (1). Notes: A current Microsoft NT Server license is required (end-user must provide serial number).

CAD-2 NAVAIR/SPAWAR
Vehicle: N66032-94-D-0012
Intergraph
POC: Bob Donahue (301) 757-9146
CLIN/BLIN: 03BB11
Description: MS Windows NTW Workstation (V4.0) for non-Intergraph Microsoft Windows NT is the 32-bit, multithreaded, multitasking operating system for Intel-based workstations. SH**265 is Microsoft Windows NT Workstation version 4.0 with support for up to two processors. BSM level support includes version upgrades plus phone support assistance with installation, configuration and trouble-shooting the use of:

- NTW operating system,
- Intergraph drivers (SCSI, video and network) and HAL,
- Network protocols (NetBEUI, TCP/IP, DLC, NWLink IPX/SPX, and DHCP, and connectivity,
- Services: Netware client, RAS, WINS, and DHCP, and 5) printer/peripheral
- drivers for devices purchased from Intergraph. Also error message interpretation for NTW and drivers. NTW "bug" reporting to Microsoft. Driver bug reporting to Intergraph with fixes provided via IBBS/ftp/www site.

CLIN Part Number(s): SHBY265AA-0400A - Microsoft NT Workstation S/W for CAD-2

CLIN/BLIN: 03BC11
Description: MS Windows NTW Workstation (V4.0) for non-Intergraph (License only). Microsoft Windows NT is the 32-bit, multithreaded, multitasking operating system for Intel-based workstations. SH**265 is Microsoft Windows NT Workstation version 4.0 with support for up to two processors.

CLIN Part Number(s) SHBY265AA-0400A - Microsoft NT Workstation S/W For CAD-2

CAD-2 NAVSEA

Vehicle: N66032-91-D-0003
Intergraph
POC: Craig Carlson (703) 602-5556
CLIN/BLIN: S005NFA
Description: MS Windows NT Workstation V4.0 (Non-Intergraph Workstation) (Complete Package). Microsoft Windows NT Workstation is the NT operating system software provided for Intel-based PCs and Workstations. NOTE: The software installation clause of this contract is waived for this product. This CLIN is version-specific; subsequent versions will be added by mutual agreement.

Monthly Maintenance

Prerequisites: Users wishing to purchase phone support must purchase either the complete package or license only CLIN from this contract to qualify.

CLIN Part Number(s): SHBY265AA-0400A - Microsoft NT Workstation S/W for CAD-2

S005NFAP - MS Windows NT Workstation

CLIN/BLIN: S005NNA
Description: MS Windows NT Workstation V4.0 (Non-Intergraph Workstation) (License only). Microsoft Windows NT Workstation is the NT operating system software provided for Intel-based PCs and Workstations. This CLIN is provided as license only and includes a 30-day media warranty. Prerequisites - Users wishing to purchase phone support must purchase CLIN S005NNAP.

CLIN Part Number(s) - SHBY265AA-0400A - Microsoft NT Workstation S/W for CAD-2

S005NNAP - Monthly Maintenance

NTOPS
Vehicle: N68939-96-D-0007
TRACOR
POC: Lyn Purvis (619) 524-7541
http://cad2.www.cordant.com/ntops/ntops.htm
CLIN/BLIN: 0041FD
Description: MS Windows 95 Upgrade (Floppy Disk Media). The Multi-Processing Operating System Windows 95 Upgrade is a 32-bit operating system that executes multiple application programs. Notes: If this SLIN is ordered with any Desktop or Notebook, Windows 95 will be installed rather than Windows for Workgroups 3.11 & MS-DOS 6.22.

CLIN/BLIN: 0041CD
Description: MS Windows 95 Upgrade (CD-ROM Media). The Multi-Processing Operating System Windows 95 Upgrade is a 32-bit operating system that executes multiple application programs. Notes: If this SLIN is ordered with any Desktop or Notebook, Windows 95 will be installed rather than Windows for Workgroups 3.11 & MS-DOS 6.22.

CLIN/BLIN: 0049CD
Description: MS Windows NT Workstation OS (CD-ROM Media). MS Windows NT Workstation Operating System (CD-ROM Media) provides the end-user with the foundation to work in a multi-processing environment. Using the capabilities of a 32-bit multi-tasking operating system and symmetric multiple processing (SMP) support, Windows NT Workstation can handle

more resource intensive tasks. In addition, it is configurable to integrate into existing networks with built-in driver support for TCP/IP and IPX/SPX protocols.

FISC Philadelphia
Vehicle: N00140-97-A-3692
GTSI
POC: Dorothy Hennigan (757) 322-3998
CLIN/BLIN: 8020
Description: Windows NT Workstation 4.0 English Disk Kit CD R0M Boot Disks. MFG PN: 236-00036; GTSI PN: 3494-122451

CLIN/BLIN: 8021
Description: Windows NT Workstation 4.0 English NA DocKit. MFG PN: 236-00037; GTSI PN: 3494-122442

CLIN/BLIN: 8023
Description: Windows NT Workstation 4.0 Competitive Product Upgrade. MFG PN: 236-074V40VL; GTSI PN: 3493-123532

CLIN/BLIN: 8024
Description: Windows NT Workstation 4.0 Upgrade from Windows NT 3.X. MFG PN: 236-274-40VL; GTSI PN: 3493-123533

CLIN/BLIN: 8025
Description: Windows 95 Version Upgrade from Windows 3.X. MFG PN: 060-050-95VL; GTSI PN: 3493-123424

CLIN/BLIN: 8026
Description: Windows 95 English Disk Kit 3.6. MFG PN: 050-031-918; GTSI PN: 3494-122389

CLIN/BLIN: 8027
Description: Windows 95 English DocKit. MFG PN: 050-030-900; GTSI PN: 3494-122340

CLIN/BLIN: 8028
Description: Windows NT Workstation 1-Time Upgrade Win, Win 95, Windows for Workgroups. MFG PN: 236-00558; GTSI PN: 3494-123605

CLIN/BLIN: 8036
Description: Windows NT Server 4.0 License. MFG PN: 2273276V40VL; GTSI PN: 3493-123541

CLIN/BLIN: 8042
Description: Windows 95 Version Upgrade from Windows 3.x. MFG PN: 050-050-95VL; GTSI PN: 3493-123424

CLIN/BLIN: 8043
Description: Windows NT Server 4.0 English NA Disk Kit NA Only CD-ROM w/Boot. MFG PN: 227-00284; GTSI PN: 3494-122450

ViViD
Vehicle: N68939-97-D-0041
GTE
POC: David Mullins (619) 524-7538

CLIN/BLIN: XXXX
Description: JAVA - Proposal under evaluation

CLIN/BLIN: XXXX
Description: JAVASCRIPT - Proposal under evaluation

CLIN/BLIN: XXXX
Description: MS Windows NT Client Access - Proposal under evaluation

CLIN/BLIN: XXXX
Description: MS Windows NT Server - Proposal under evaluation

CLIN/BLIN: XXXX
Description: MS Windows NT Workstation - Proposal under evaluation

ViViD
Vehicle: N68939-97-D-0040
Lucent
POC: David Mullins (619) 524-7538
CLIN/BLIN: XXXX
Description: JAVA - Proposal under evaluation

CLIN/BLIN: XXXX
Description: JAVASCRIPT - Proposal under evaluation

CLIN/BLIN: XXXX
Description: MS Windows NT Client Access - Proposal under evaluation

CLIN/BLIN: XXXX
Description: MS Windows NT Server - Proposal under evaluation

CLIN/BLIN: XXXX

Appendix E – Release Notes

Reserved for Future Use.

Appendix F – Record of Changes

Reserved for Future Use.

Appendix G – Bibliography

The DON ITSG is founded upon several Department of Defense (DoD), Defense Information Systems Agency (DISA) and Department of the Navy (DON) directives and documents. The framework is based upon specifications, standards, guidance and best practices found in government, educational, commercial, and international technical literature. For quick reference, each DON ITSG Chapter contains a list of documents used in creating the chapter or that could be useful to the reader. The Bibliography compiles the list of references used in alphabetical order and sets the foundation documents apart from the remaining technical references.

The references are listed in alphabetical order per the following format:

Author *(if known)* (Author's Organization or Organization Producing the Reference); "Title of the Reference" or *Book Title*, Date of the Reference, Publisher *(if applicable)*, URL (date of access), {Where the reference is cited in the ITSG}

Note that references cited as "Internet Drafts" expire in six months.

Product and company names mentioned herein may be privately owned trademarks. Reference to them in the bibliography does not imply endorsement or recommendation by the Government. In this context they are used as sources of information.

Foundation Documents

Information Technology Management Reform Act of 1996 (ITMRA 96) http://www.dtic.mil/c3i/cio/references/itmra/itmra.Annot.html (24 May 1998)

Department of Defense(DoD*) Joint Technical Architecture*, Version 1.0, 22 August 1996, UNCLASSIFIED (Draft Version 2.0 of 28 July 1998 is available for comment through http://www-jta.itsi.disa.mil/).

Department of Defense (DOD); *Information Technology Standards Guidance (ITSG) -- Version 3.1;* 7 April 1997, www-itsg.itsi.disa.mil/itsg_v31.htm (23 May 1998)

Joint Staff, J6, "C4I For the Warrior" 12 June 1992

Joint Staff, "Joint Vision 2010, America's Military: Preparing for Tomorrow"; 1996

Chief of Naval Operations (CNO) N6 Copernicus: C4ISR for the 21st Century, September 1997

U.S. Marine Corps "...From the Sea" September 1992

Defense Information Systems Agency (DISA): Joint Defense Information Infrastructure Control Center Concept of Operations (DII CC CONOPS); 22 July 1996

Defense Information Systems Agency (DISA); "Defense Information Infrastructure Common Operating Environment (DII COE);" 1 May 1998; http://spider.osfl.disa.mil/dii/ (24 May 1998)

SPAWAR Systems Center San Diego; "Navy C4ISR Technical Architecture" Version 0.9; 17 September 1997.

Technical References

These references are available at the end of each chapter.

Appendix H - Acknowledgments

The DON CIO ITSG Document was written by a committee which included the DON ITSG IPT, members of the DON CIO Staff, and ad hoc DON personnel who provided their time and effort to create a useful product. This attempts to acknowledge the works of the most significant contributions.

Shown is a list of people on the left followed by their organization. On the far right is their area of contribution to the ITSG. Bold indicates that the individual was the primary contributor.

The DON CIO ITSG IPT

Chairperson:		
Mr. Randy Cieslak,	SPAWAR Systems Center San Diego in support of Commander in Chief, U.S. Pacific Fleet	**Chapter 1** **Chapter 2** **Chapter 10** **Appendix C** **Appendix E** **Appendix G**
Members:		
Mr. Gary Bean	USMC MCCDC	Advisor
Mr. Luther Blackwell	Naval Sea Systems Command	**Chapter 4** Chapter 5 Chapter 10
Mr. Rex Buddenburg	Naval Post Graduate School	Advisor Chapter 5 Chapter 10 **Appendix A** **Appendix B**
Mr. Kar Chan	Space and Naval Warfare Systems Command	Advisor
Mr. Basil Decina	Naval Research Lab	**Chapter 5** Chapter 2
Dr. Kathy Fernandes	SPAWAR Systems Center San Diego	Chapter 7
LCDR Chris Gedo	Space and Naval Warfare Systems Command	Chapter 5 Chapter 6 Chapter 9
Mr. Will Gex	SPAWAR Systems Center Charleston	**Chapter 7**
Mr. Tony Ho	Commander in Chief, U.S. Pacific Fleet	Chapter 5 Chapter 9
Mr. Bob Johnson	Chief of Naval Operations, N4	Chapter 5 Chapter 7
Mr. Phil Johnson	Naval Research Lab	Chapter 5
Mr. Russ Jones	Chief of Naval Operations N6	Chapter 10
Mr. Dave Mihelcic	Naval Research Lab	**Chapter 3**
Mr. Gerry Mullins	Commander-in-Chief, U.S. Atlantic Fleet	Chapter 4 Chapter 10
Mr. Greg Michaels	GRCI in support of Chief of Naval Operations N6	**Chapter 8**
Ms. Linda Salisbury	USMC	Chapter 9
Mr. Mike Randall	Naval Air Systems Command	**Chapter 6**

Mr. John Rivers	Naval Sea Systems Command	Chapter 2 Chapter 5
Mr. David Townsend	Navy Research Lab	Chapter 5
Mr. Mark Williams	Chief of Naval Operations N4	Chapter 7
Mr. Merrill Witzel	SPAWAR SYSCEN SD in support of Commander in Chief, U. S. Atlantic Fleet	**Chapter 9**
Mr. Lee Zimmerman	SPAWAR Systems Center San Diego	Chapter 6 Chapter 9

DON CIO ITSG IPT Support Staff

Mr. Dale Christensen	DON CIO Staff	Advisor
Mr. Floyd Groce	DON CIO Staff	**Appendix D**
Ms. Penny Jones	DON CIO Staff	Facilitator
Mr. Richard Lynch	DON CIO Staff	Technical Advisor
Ms. Judy McCarthy	DON CIO Staff	Facilitator
Ms. Karen Overall	EDS in support of DON CIO	**Lead Editor**
Mr. Tom Scruggs	EDS in support of DON CIO	**Lead Coordinator**

EDS Support Staff

Mr. Bill Purcell	EDS	Editor
Mr. Tom Arnette	EDS	Advisor
Mr. Dick Parodi	EDS	Advisor
Mr. Hank Pusser	EDS	Advisor
Mr. Matt Constantine	EDS	HTML Designer

The DON CIO ITSG IPT wishes to thank the following colleagues who made significant contributions:

Mr. F. J. Garner	Naval Surface Warfare Center, Carderock Division	Chapter 8
Mr. Lew Gutman	Space and Naval Warfare Systems Command	Chapter 5 Chapter 10
Mr. Richard Hale	Naval Research Lab	Chapter 3
Mr. Scott Henderson	Space and Naval Warfare Systems Command	Chapter 3
Dr. Bernie Schneiderman	SPAWAR Systems Center San Diego	Editor
Mr. Skip Thaeler	Space and Naval Warfare Systems Command	Chapter 3
Mr. Jack Wilson	SPAWAR Systems Center San Diego	Advisor
Mr. Marc Apter	Naval Sea Systems Command	Chapter 3
Major Roger Ashworth	USMC (AC/S C4I)	Chapter 3
CDR Tod Brethauer	Chief of Naval Operations N2 Staff	Chapter 5
Mr. Craig Carlson	Naval Sea Systems Command	Chapter 5
Mr. Earl Demastro	NAWCAD Depot Cherry Point	Chapter 7
Mr. R.W. Etter	NSMA	Chapter 7 Chapter 10
Mr. Sam Katz	Commander in Chief, U.S. Atlantic Fleet	Chapter 6
Mr. Ken Kelson	SAIC, Inc. in support of Commander in Chief, U.S. Pacific Fleet	Figures

Mr. Stephen Kuba	SPAWAR Systems Activity Pacific	Chapter 4 Chapter 9
Mr. Kent Kuriyama	SPAWAR Systems Center San Diego in support of Commander in Chief, U.S. Pacific Fleet	Chapter 6
Mr. Vince Lee	Commander in Chief, U.S. Pacific Fleet	Chapter 5 Chapter 9
Mr. Wren Lee	Netelegence, Inc. in support of Commander in Chief, U.S. Pacific Fleet	Chapter 5
Ms. Marthann McTighe	Naval Computer & Telecommunications Command	Chapter 3
LCDR Al Pepper	Commander in Chief, U.S. Atlantic Fleet	Chapter 5
Mr. Paul Stenger	Naval Medical Information Management Center	Chapter 5