Document Number 102-94-022U

Technical Report

Naval Network Security Requirements Analysis

Task 4
Contract No. N00039-93-C-0099
CDRL No. A003

December 7, 1994

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037
(619) 546-8616

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 7, 1994	Final

4. TITLE AND SUBTITLE
Technical Report
Naval Network Security Requirements Analysis

5. FUNDING NUMBERS
Contract No:
N00039-93-C-0099

6. AUTHOR(S)
Kym Blair

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037

8. PERFORMING ORGANIZATION REPORT NUMBER
102-94-022U

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71)
Arlington, Virginia 22245-5200

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement: Approved for Public Release; Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Secure Solutions, Inc. was tasked by the Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II network security research effort. The report analyzes the DoD Goal Security Architecture (DGSA), Multilevel Information System Security Initiative (MISSI), and Navy Integrated Command and Control, Communications and Computers, and Intelligence (Integrated C4I) program areas in order to determine security implementation requirements for Navy networks.

The report describes broad network security requirements for the Navy in light of emerging technologies. The analysis includes a brief review of the current environment, characterized by existing and emerging network security products, and discusses possible deficiencies which may require the development of additional security products. These findings are preliminary and merit further investigation.

14. SUBJECT TERMS	15. NUMBER OF PAGES
	110
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements***.

Block 1. Agency Use Only *(Leave blank)*.

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C	- Contract	**PR**	- Project
G	- Grant	**TA**	- Task
PE	- Program Element	**WU**	- Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

- **DOD** - See DoDD 5230.24, "Distribution Statements on Technical Documents."
- **DOE** - See authorities.
- **NASA** - See Handbook NHB 2200.2.
- **NTIS** - Leave blank.

Block 12b. Distribution Code.

- **DOD** - Leave blank.
- **DOE** - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
- **NASA** - Leave blank.
- **NTIS** - Leave blank.

Block 13. Abstract: Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only)*.

Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

*U.S.GPO:1993-0-353-779

Document Number 102-94-022U

Technical Report

Naval Network Security Requirements Analysis

Task 4
Contract No. N00039-93-C-0099
CDRL No. A003

December 7, 1994

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037
(619) 546-8616

Approved for public release; distribution is unlimited.

This Page Intentionally Left Blank

Table of Contents

Appendices

Appendix **Page**

Index of Figures

Figure **Page**

Index of Tables

Table **Page**

Executive Summary

Secure Solutions, Inc. was tasked by the Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II network security research effort. This Task 4 report analyzes the DoD Goal Security Architecture (DGSA), the Multilevel Information Systems Security Initiative (MISSI), and the Navy Integrated Command and Control, Communications and Computers, and Intelligence (Integrated C4I) programs in order to determine security implementation requirements for Navy networks in light of emerging technologies.

The study identifies 10 major security implementation requirements. They are to provide security for the following:

- Open systems architecture
- Interconnectivity and distributed processing
- Use of COTS / GOTS hardware and software
- Processing at extremely high speeds
- Multilevel security
- User mobility
- Multimedia communications
- Firewalls
- Selectable security services
- Multicast routing

The analysis includes a brief review of the current environment, characterized by existing and proposed network security products, and discusses possible deficiencies which may require the development of additional security products. These findings are preliminary and merit further investigation.

The major conclusions of this Task 4 study are that it appears there are not adequate security products to meet the requirements for:

- Secure User Mobility – As networks become more robust and users become more mobile, users will demand access to their data from any station in the network. As computers become more portable, they will at times require broadcast media for connectivity to the network rather than cables. Likewise, when a computer is carried around a ship, aircraft, hospital, or other workplace, the connection must not be lost or interfered with, and must not interfere with other signals such as radar and navigation. Technology is beginning to address the need for mobility, but security has not been a driving force in the development efforts.

- Secure Multimedia – Some trusted workstations are able to apply two types of sensitivity labels to the information they represent, one that indicates the classification range for the user and one that indicates the sensitivity of a particular window. The label for the information will be at the same or lower sensitivity level as the user's session label. Network security mechanisms also indicate a workstations range of permissible classifications and the classification level for a particular session, but no single protocol has been designed to handle both. Multimedia communications will require such labeling. There are other security issues that pertain to multimedia. In particular, as multimedia applications are introduced to run at the speeds of ATM, the minimum acceptable transmission speeds will rise rapidly. Security mechanisms must be developed to support these speeds. Some SONET and ATM encryptors are being developed, but encryptor products are needed at higher layers as well.

- Secure Firewalls – The security community is not in agreement as to whether firewalls are beneficial or detrimental. Some argue that firewalls provide a false sense of security. Since, by definition, some protocols must be permitted to pass traffic through the firewall, that traffic can be dangerous and difficult to protect. Others argue that firewalls can filter out specific types of communications that are known to be high risk. Regardless, firewalls are not currently very effective. Since it is not presently possible to install adequate security in every user workstation and server, and since interconnectivity is needed for operational purposes, there is presently an urgent need for secure firewalls.

- Secure Multicast Routing – In order to minimize network congestion, multicast techniques are being developed to send one copy of a message across parts of the network and then have routers burst the message into multiple copies for delivery to all intended recipients. This capability is imperative as multimedia applications become more common. This capability is also imperative as communication bandwidths to and from mobile platforms (e.g., ships) are always less than desired. As multicast protocols are developed, security issues must be addressed to ensure that routers correctly deliver traffic to all intended users and at the same time do no deliver traffic where it is not intended. Other security implications concern the application of security protocols that encrypt the destination address in a protected header. Since the multicast protocol must be able to modify the address entries, it may conflict with the use of an end-to-end security protocol.

Since the technologies and standards that support mobile users and multicast capabilities are not stable, it may be premature to attempt to develop security products for these areas. However, participation in the standardization efforts by security engineers is highly recommended. Security products should be developed to meet near-term requirements for the following:

- Secure Multimedia – Multimedia applications are being developed and will soon be in wide use on internetworks. Existing mechanisms that provide security

services are not suitable for the wide bandwidth of multimedia, or for providing unique security such as supporting multiple sensitivity labels for video and whiteboard windows. Whiteboard windowing is a service that generally piggybacks on video teleconferencing to provide a second window that displays the speaker's presentation slides. The audience can then simultaneously view the speaker and the slides. An advantage of whiteboarding is that it uses a narrow bandwidth to provide the service.

- Secure Firewalls – Several types of firewalls are urgently needed. Perhaps the most important are Network Layer firewalls (routers). However, there may also be requirements for Data Link Layer firewalls (bridges) or for application specific firewalls that could be installed in-line with the current generation of router firewalls.

Further studies are needed to assess these areas that appear to be deficient. Additional products are needed to meet the security needs in these two areas. When user mobility and multicast technologies are more stable, security protocols, products, and interfaces will be needed in those areas.

This Page Intentionally Left Blank

Section 1

Introduction

This Page Intentionally Left Blank

1.0 Introduction

This task 4 report documents the results of an analysis performed by Secure Solutions under the Small Business Innovation Research (SBIR) Program for the Department of the Navy's Space and Naval Warfare Systems Command (SPAWAR) under Contract Number N00039-93-C-0099. The report describes broad network security requirements for the Navy in light of emerging technologies.

This introduction provides background information on why this research effort was initiated, the scope and objectives of the study, the approach used, and the organization of the report.

1.1 Background

Admiral Jerry Tuttle, when Chief of Naval Operations, stated, ***"I have become convinced that command and control – which, when welded to technology, becomes command and control, communications and computers, and intelligence (C^4I) – will represent the true revolution in naval warfare of our generation. Modern navies are inextricably tied to technology, which applies to weapons and platforms, delineates battle space and allows innovative men and women to develop the tactics of warfare within it. So alluring is this technology, so quickly has it come upon us, that we have virtually reorganized the Navy over it. Technologically, this will mean a new C^4I system that can provide the tactical commander with the means to increase his span of command and control up into space and beyond the 500-mile limit of the current air, surface and subsurface dimensions."*** [DIGIRO 91]

Indeed, technological advances have created new opportunities for sharing huge quantities of information at very high speeds. Information is no longer centralized within a few organizations on a few mainframes. It is now distributed across wide networks that tie together the computers of many organizations. New approaches are needed for describing ownership and control responsibilities for information. New approaches are needed for applying security to information.

Two important Department of Defense (DoD) program areas are being supported by the National Security Agency (NSA) and the Defense Information Systems Agency (DISA) to provide structure to future information processing system security needs. The first is the DoD Goal Security Architecture (DGSA). The DGSA is a high level framework for Defense Information System (DIS) operational environment security architectures. The DIS will eventually provide writer-to-reader messaging, among other services. Its development is predicated upon the worldwide interconnection of user workstations. The DGSA specifies security principles and target security capabilities to guide system security architects in creating specific security architectures that are consistent with the DGSA, but it does not provide specifications for particular information systems or components. The DGSA is intended to be generic and flexible so that specific operational systems may be developed to satisfy specific operational missions. Figure 1-1 depicts the DGSA.

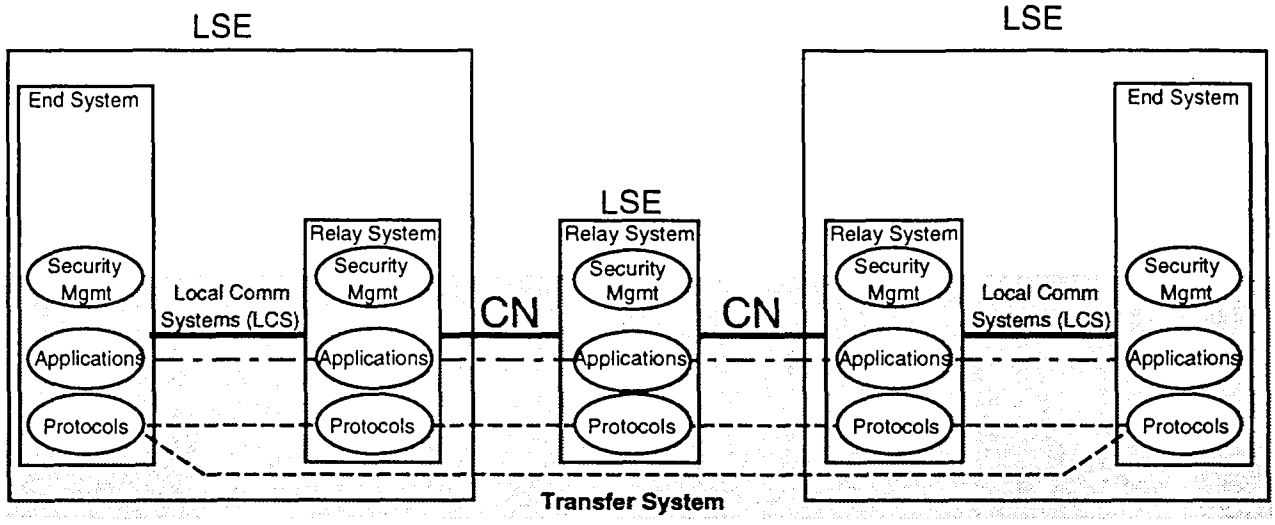


Figure 1-1. DoD Goal Security Architecture (DGSA) Configuration

The primary components of the DGSA are the Local Subscriber Environment (LSE) and the communications network (CN). LSEs are mission-oriented. Rules, policies, and authorities are established to define an LSE. Certifications and accreditations are required for each security policy that an LSE will support. For an LSE to be permitted to support multiple security policies, it must be accredited by the organizations that are responsible for the policies. As shown in Figure 1-1, an LSE can consist of end systems, relay systems, or end systems, local communications systems (LCSs), and relay systems. The DGSA defines a transfer system which consists of LCSs, CNs, networking applications, communications protocols, and security management information databases implemented in end systems and relay systems. It is responsible for providing network security services across the network.

The second program area that is being developed by NSA and DISA is the Multilevel Information Systems Security Initiative (MISSI). The objective of MISSI is to transition multilevel security from its current state, where there are few products that can be used to construct secure computer networks using existing unclassified backbones, to a state where there is a suite of products that provide network security services for communications over unclassified backbones. In addition to providing secure organization-to-organization communications over unclassified backbones, MISSI will support secure writer-to-reader communications over unclassified backbones.

Current plans for the MISSI family of products include a Secure Network Server (SNS) which implements the Logical Coprocessing Kernel (LOCK™) in a workstation, a workstation peripheral implemented with Personal Computer Memory Card International Association (PCMCIA) "smart card" technology, internal workstation security products, a workstation In-Line Network Encryptor (INE), and a Network Security Manager (NSM) control workstation. MISSI documentation does not refer to LSEs. However, the MISSI components can be thought of in terms of LSEs (consisting of end systems, LCSs, and relay systems) and CNs. Figure 1-2 depicts the MISSI architecture configured as LSEs

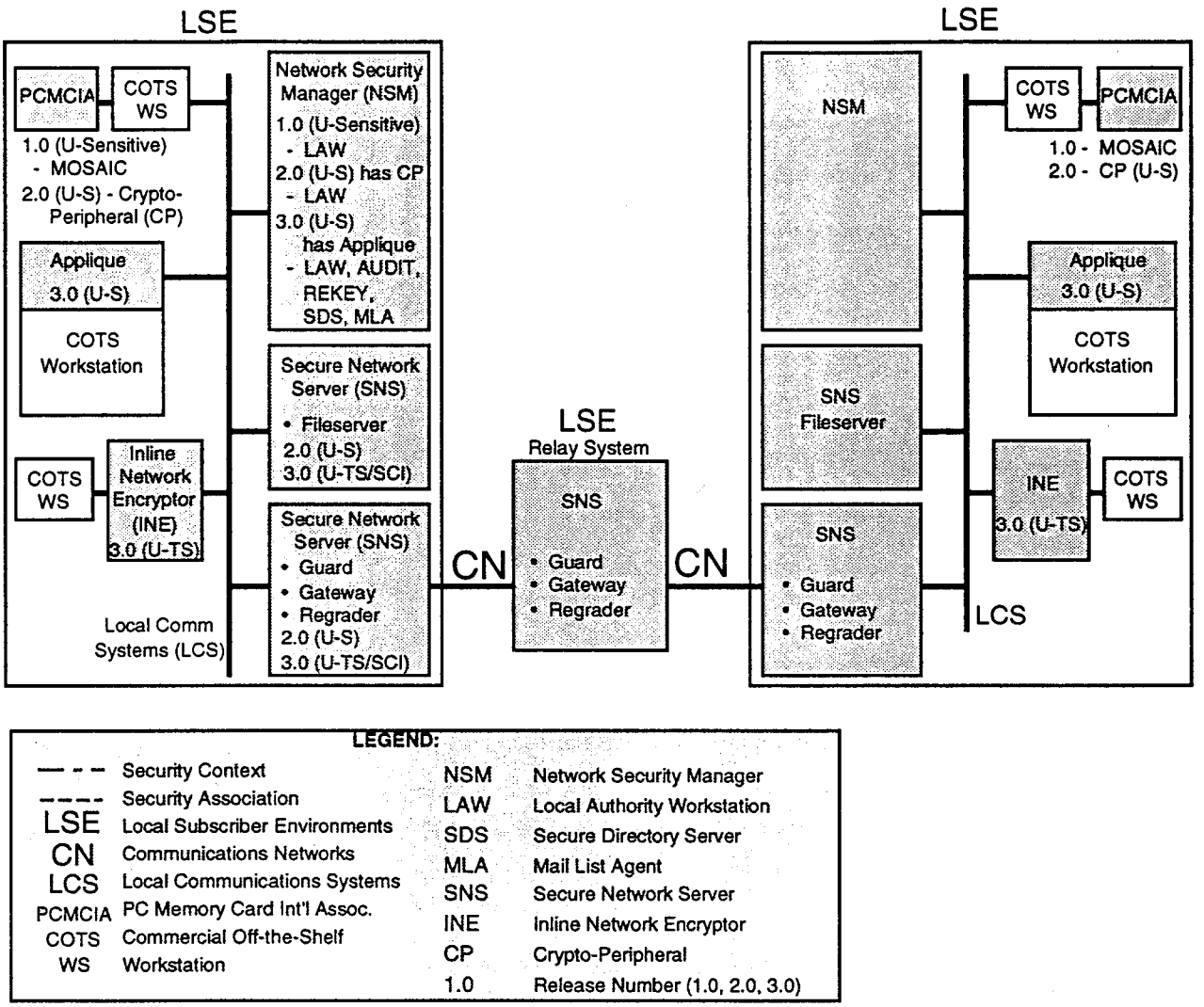


Figure 1-2. Multilevel Information Systems Security Initiative (MISSI) Architecture

and CNs. As can be seen, MISSI components could be selected by Navy network system implementors to achieve the DoD Goal Security Architecture.

In addition to the DGSA and MISSI program areas, the Navy is developing an operational environment known as Integrated command and control, communications and computers, and intelligence *(Integrated C4I),* formerly *Copernicus.* Integrated C4I is a broad technological, doctrinal, and organizational infrastructure that provides C4I capabilities to support the Naval Space and Electronic Warfare (SEW) mission. Integrated C4I encompasses *warfare support* and *warfare* disciplines. The Integrated C4I Architecture, shown in Figure 1-3, is based on four pillars: the Global Information Exchange Systems (GLOBIXS), the CINC Command Complex (CCC), the Tactical Data Information Exchange Systems (TADIXS), and the Tactical Command Center (TCC).

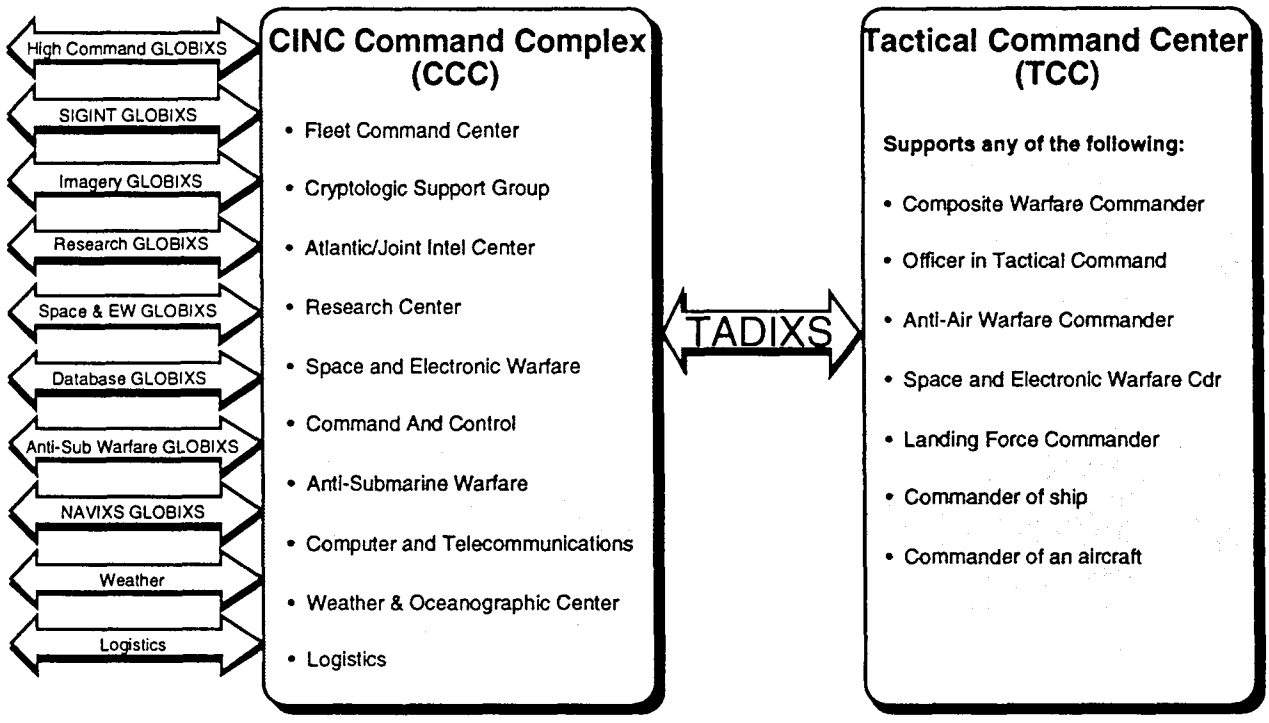


Figure 1-3. The Integrated C4I Architecture

CCCs incorporate virtual networks consisting of many local area networks (LANs) connected by a metropolitan area network (MAN). CCCs will be established at a few locations around the world. TCCs will support tactical commanders such as commanders of carriers, submarines, aircraft, land forces, and joint task forces. Tactical level TCCs are analogous to theater level CCCs. The TCC provides the tactical connectivity to units and other force commanders.

GLOBIXS are shore-based worldwide virtual networks supported by the Defense Communications System (DCS) and commercial networks. GLOBIXS will provide strategic connectivity among government agencies and industry. TADIXS are afloat virtual networks that provide tactical communications to a wide variety of user communities and are implemented over Communications Support System (CSS) assets using shared HF, VHF, UHF, SHF, EHF military satellite, and commercial satellite circuits.

All three program areas, DGSA, MISSI, and the Navy Integrated C4I, will take advantage of technological advances in order to provide large-scale interconnectivity between DoD organizations. All three program areas have unique, but closely related, security implementation requirements which are of importance in the Naval environment.

1.2 Scope

This Task 4 study analyzes the DGSA, MISSI, and Navy Integrated C4I program areas in order to determine security implementation requirements for Navy networks. Each program area is evaluated separately, then the resulting requirements are combined into a composite list of high-level requirements.

The analysis includes a brief review of the current environment, characterized by existing and emerging network security products, and discusses possible deficiencies which may require the development of additional security products. These findings are preliminary and merit further investigation.

1.3 Study Objectives

The objective of task 4 is to identify the high-level security implementation requirements for Navy networks. The results may be used as a basis for future studies that fully characterize the current environment and focus on strengths and deficiencies in security products in order to identify areas where additional security products are needed by the Navy.

1.4 Approach

This study was accomplished by performing the following steps:

- Determining the threat to Navy information systems and networks, which is the basis for the security policy
- Reviewing the security policy, which is the basis for the security requirements, and assessing the risk
- Analyzing the DoD Goal Security Architecture to determine network security implementation requirements
- Analyzing the Multilevel Information Systems Security Initiative (MISSI) documentation to determine network security implementation requirements
- Analyzing the Integrated C4I documentation to determine network security implementation requirements
- Combining the three lists of security requirements into a single brief list of high-level network security implementation requirements
- Briefly reviewing network security product design documentation and characterizing the existing security environment at a very high level
- Suggesting what areas do not appear to have sufficient security mechanisms proposed to satisfy the security requirements and may merit further analysis.

1.5 Report Organization

The main body of the report is organized as follows:

- **Section 1** – Introduction
- **Section 2** – Proposed Network Security Implementation Requirements
- **Section 3** – Characteristics of Current Environment
- **Section 4** – Conclusions and Recommendations.

The following appendices are provided to supplement the main body:

- **Appendix A** – Acronyms
- **Appendix B** – DGSA Security Policy and Derived Security Requirements
- **Appendix C** – MISSI Security Requirements
- **Appendix D** – Navy Integrated C4I Security Requirements
- **Appendix E** – References.

Section 2

Proposed Network Security Implementation Requirements

This Page Intentionally Left Blank

2.0 Proposed Network Security Implementation Requirements

The basis for security requirements is a security policy that is derived from assumptions of threats to the mission. As pointed out, ***"A security policy determines the limits of acceptable behavior and what the response to violations should be."*** [CHES 94] The first step in identifying security implementation requirements is to define the threat, and then state the policy derived from the threat. The Joint Security Commission's *Redefining Security: Report to the Secretary of Defense and the Director of Central Intelligence* [JSC 94] describes the treat as follows:

> ***Thirty years ago, computer systems presented relatively simple security challenges. They were expensive, isolated in environmentally controlled facilities, and their use was an arcane art understood by few. We used worst case scenarios as the basis for most of our security planning. As size and price came down, microprocessors began to appear in the workplace, in homes, and on the battlefield. The threats today are more diffuse, multifaceted, and dynamic.***
>
> ***Networks are recognized as a battlefield of the future. The threat to our information and information systems is increasingly sophisticated, and comes from both insiders and outsiders.***
>
> ***Attacks against information systems are becoming more aggressive, not only seeking access to confidential information, but also stealing and degrading service and destroying data. Computer viruses are growing more common and more dangerous and may be undetectable by conventional antiviral software. Over 4,000 hacker attacks were detected on one unclassified government system during a single three month period.***
>
> ***Terrorists' use of weapons of mass destruction, or an adversary's foreknowledge of our battle plans, could have consequences so grave as to demand the highest reasonably attainable standard of security. Highest priority is given to limiting the proliferation of weapons of mass destruction and advanced conventional weapons. Increasingly cheaper and more powerful commercially available electronics put signals intelligence intercept and processing capabilities within the reach of the smallest countries and even drug traffickers. Policymakers are focusing on the threat from foreign governments and nongovernment entities to US advanced technologies, defense-related industries, proprietary data, intellectual property rights, and trade secrets.***
>
> ***Eighty-five percent of computer crime is committed by insiders with validated access to the systems and networks they abuse. Because the government is so completely dependent on cleared personnel to safeguard classified information, the personnel security system is at the very heart of the government's security mission. Without adequate personnel screening, the rest of the security mission would be a worthless facade and a waste of resources. Recent history is regrettably all too rich in proof of the damage that a single cleared person can cause.***
>
> ***It is possible to balance the risk against the costs of countermeasures. We can and must provide a rational, cost-effective, and enduring framework using risk management as the underlying basis for security decisionmaking.***

The JSC report goes on to say that policies and standards are not suitable for the networked world of today because they were developed when computers were physically and electronically isolated. The report states that, ***"The Commission believes***

that information systems security policy must better address current and future electronic environments. The network architecture of the future will comprise a seamless global web of unsecured electronic highways linked together to provide a common infrastructure operated as a utility."

The National Security Agency (NSA) and the Defense Information Systems Agency (DISA) have developed the *DoD Information Systems Security Policy* [NSA 93A] which is summarized in the *DoD Goal Security Architecture* [DGSA 93] as follows:

1. ***DoD information systems must support information processing under multiple security policies of any complexity or type, including those for sensitive unclassified information and multiple categories of classified information.***
2. ***DoD information systems must be sufficiently protected to allow distributed information processing (including distributed information system management) among multiple hosts on multiple networks in accordance with open systems architectures.***
3. ***DoD information systems must support information processing among users with different security attributes employing resources with varying degrees of security protection, including users of nonsecure resources if a particular mission so dictates.***
4. ***DoD information systems must be sufficiently protected to allow connectivity via common carrier (public) communications systems.***

The security required to support future visions of data automation were viewed from three perspectives, all of which are compatible. First, security implementation requirements were extracted from the DoD Goal Security Architecture (DGSA). The DGSA is a high level framework for security architectures in the operational environment for the Defense Information System (DIS). In developing the DGSA, consideration was given to the protection of information and system assets as part of the total view of the missions, threats, performance, interoperability, extensibility, useability, and cost of implementation. The DGSA guides system security architects in creating specific security architectures, but it does not provide information systems or component specifications.

Second, security implementation requirements were extracted from the Multilevel Information Systems Security Initiative (MISSI). The objective of MISSI is to transition multilevel security from its current state, where there are few products that can be used to construct secure computer networks using existing unclassified backbones, to the DGSA, where a suite of products will provide confidentiality, access control, non-repudiation, data integrity, and data origin authentication for electronic mail, file transfer, and multimedia services from writer-to-reader. As such, MISSI and DGSA are well coordinated and extremely compatible. Both are intended to be evolutionary and flexible. Evolutionary in that each involves a series of phases that are increasingly more secure. Flexible in that various approaches and products can be implemented and tailored to meet a variety of security policy environments. The goal of MISSI is to

provide multilevel security for all operational environments including each of the DoD service environments. Specifically, the Navy's operational environment for information processing and communications is known as Integrated command and control, communications and computers, and intelligence *(Integrated C4I),* formerly *Copernicus.*

Finally, security implementation requirements were extracted from documentation that describes the *Integrated C4I* security architecture. Admiral Jerry Tuttle, former Chief of Naval Operations, had stated, ***"The Copernicus Architecture marks a revolution in Navy Command, Control, Communications, Computers and Intelligence (C4I) - the first successful top-down restructuring undertaken since World War II. The Copernicus Architecture with its attendant Investment Strategy, will eliminate the critical shortcomings highlighted during Desert Storm and give us the technological means to move Space and Electronic Warfare (SEW) into the 21st Century. It is my desire that nothing stand in our way in implementing Copernicus and that all C4I programs within Navy be moved under its architectural and programmatic aegis soonest."*** [CNO 93]

Integrated C4I is a broad technological, doctrinal, and organizational infrastructure that provides C4I capabilities to support the Naval Space and Electronic Warfare (SEW) mission. Integrated C4I encompasses **warfare support** (support for friendly troops) and **warfare** (against the enemy) disciplines. These disciplines are as follows:

Warfare Support	Warfare
Operational Security	Operational Deception
Surveillance	Counter-surveillance
C4I	Counter-C4I
Signals Management	Electronic Combat

The three security program areas were first evaluated separately to identify important security implementation requirements. The security implementation requirements that were extracted for this report were stated or inferred in the source documentation. The high level DGSA, MISSI, and Naval Integrated C4I security implementation requirements and their sources are identified in Appendices B, C, and D, respectively. The three sets of security implementation requirements were consolidated into a complete set of high-level security implementation requirements that indicate the direction of Naval security initiatives for the future. This three-tier perspective is depicted in Figure 2-1.

The high-level DGSA, MISSI, and Naval Integrated C4I security implementation requirements are shown in Table 2-1. The requirements are arranged into 10 categories, as discussed in Sections 2.1 through 2.10. Foremost among the security requirements are the need for secure open systems, interconnectivity and distributed

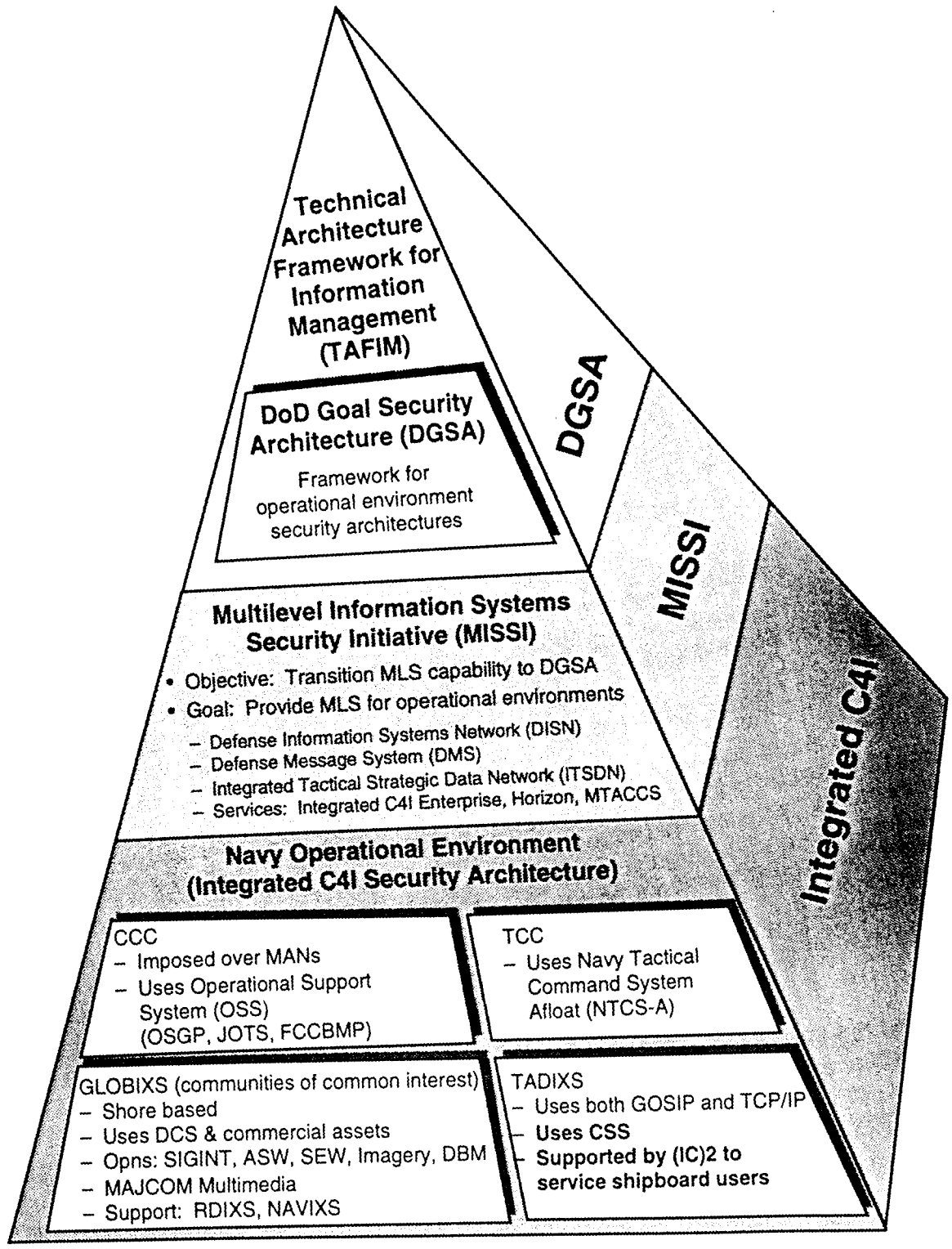


Figure 2-1. Foundation of Data Automation Security Requirements

Table 2-1. Proposed Security Implementation Requirements (Page 1 of 3)

		DGSA	MISSI	NAVY
1	Implement open system standards	X	X	X
	– Joint-service, allied, non-allied, and commercial interoperability			
	– Establish standard component interfaces			
	– Mechanisms compatible with open systems technology			
	– Mechanisms placed where there is minimal impact on existing and anticipated applications			
	– Preserve existing application programming interfaces (APIs) to avoid changing existing applications			
	– Operate within existing network protocol standards			
	– Baseline use of TCP/IP suite. The network services include FTP (file transfer), SMTP and MSP (electronic mail), and Telnet Protocol (remote login)			
	– Evolve to widespread use of GOSIP if finalized standards, commercial technology, and a strong support base emerge			
	– BISDN networks executing GOSIP protocols are needed by the year 2010			
	– Adopt ISO 7498-2 security architecture and modifications developed by IEEE 802.10			
	– Standardize authentication information, security protocols, authorization information management, key management, and security management			
	– Standardize management protocols. SNMP version 2 and CMIP are currently best. GULS SESE and future GOSIP protocols may be better in the future			
	– Standardize format for managed object identification			
2a	Provide secure interconnectivity and distributed processing	X	X	X
	- Interface in system-high, dedicated, multilevel, and compartmented operational modes			
	- Provide connectivity between classified and unclassified systems and networks			
	- Allow connection between secure and non-secure systems			

Table 2-1. Proposed Security Implementation Requirements (Page 2 of 3)

		DGSA	MISSI	NAVY
2b	Support client-server architecture and distributed processing. Must be capable of networking mainframes, workstations, and personal computers		X	X
2c	Maintain the identities of users and information objects (classified or sensitive) under each security policy.	X	X	X
2d	Common security management is needed to manage users, security policies, information, systems, and functions that support security mechanisms. The conveyance of standard information will be the basis for decisions about what kinds of access will be authorized	X		
2e	Assure timely delivery of data. Provide reliable communications architecture to protect against denial of service. Provide survivable communications architecture which continues to function while under attack by unauthorized users	X	X	X
3	Maximize use of COTS/GOTS hardware and software	X	X	X
4	Support peak data rates in excess of 30 Mbps at some workstations			X
5	Provide multilevel secure communications and processing	X	X	X
6	Provide for secure user mobility. Allow users to access any information (from within any community necessary) required to do their job. Provide security for mobile and wireless technologies	X	X	X
7	Secure display (windows) implementation are needed for integrated multimedia (voice, imagery, data, video)	X	X	X
8	Incorporate firewalls to partition networks into communities of interest		X	X

Table 2-1. Proposed Security Implementation Requirements (Page 3 of 3)

		DGSA	MISSI	NAVY
9a	Provide selectable security services to counter a wide variety of threats (e.g., eavesdropping, modification, replay, traffic analysis, masquerade, denial of service): – Identification and Authentication – Access Control (information, services, and equipment) – Confidentiality (of user and system information) – Integrity (of information, software, and equipment) – Non-Repudiation (source and destination)	X	X	X
9b	Security labels for mandatory access control must be directly or indirectly associated with: – Each SDU exchanged as part of the service – Network entities that are clients of the service			X
9c	Provide confidence that security labels are correct (i.e., label binding and integrity mechanisms)			X
9d	Provide true user-to-user (writer-to-reader) authentication, data confidentiality, and integrity, in addition to that provided on a node-to-node basis.	X		X
9e	Maintain an audit trail to support traceability and individual accountability		X	X
9f	Provide traffic flow confidentiality for some environments	X		X
9g	Provide dynamic key management	X	X	X
10	Provide security services for multicast communications			X

processing in all operational security modes (dedicated, system high, multilevel, and compartmented), the procurement of commercial-off-the-shelf (COTS) and Government-off-the-shelf (GOTS) equipment, security in the midst of wide bandwidths, and multilevel secure (MLS) connectivity. Also of importance are requirements for secure user mobility, secure multimedia communications, security firewalls, selectable security services, and secure multicast routing of traffic.

2.1 Secure Open Systems Architecture

Open systems standards must be adopted in order to improve interoperability among joint-service systems as well as commercial systems without requiring individual host computers to have knowledge of the specific characteristics of remote host computers. Standards that describe protocols for providing security services are being adopted by standards bodies and are beginning to be used.

The long-term goal is to implement *de jure* standard protocols as specified by the International Standards Organization (ISO) and the Government Open Systems Interconnection Profile (GOSIP) [NIST 91].

Some of the ISO and GOSIP protocols have not been fully standardized nor have they been widely implemented, and they are therefore not stable. Vendors hesitate to implement products based on draft standards because standards often undergo significant revision when being upgraded from draft to international standard status. Even when standards are finalized, they are not stable. Stability comes when the standards have been implemented and there is little technological pressure to change them. Major flaws requiring correction may be discovered during implementation.

2.1.1 Near-Term Requirements

In the interim, *de facto* standard protocols which are currently implemented across a broad range of computer systems allow for a reasonable level of interoperability. This baseline suite includes Transmission Control Protocol (TCP) [RFC 81A], User Datagram Protocol (UDP) [RFC 80], Internet Protocol (IP) [RFC 81B], Simple Network Management Protocol (SNMP) [RFC 89, 90, 93A], Message Security Protocol (MSP), Simple Mail Transfer Protocol (SMTP) [RFC 82], File Transfer Protocol (FTP) [RFC 85], Telnet Protocol (remote login) [RFC 83], Carrier Sense Multiple Access with Collision Detection (CSMA/CD) [ISO 93A], Token Ring (802.5) [ISO 92A], and others. In addition, the Secure Data Network System (SDNS) family of protocols have been developed and is in use by the Government. They include Message Security Protocol (MSP) [NIST 93], Key Management Protocol [NIST 90C], Security Protocol 4 (SP4) [NIST 90A], and Security Protocol 3 (SP3) [NIST 90A].

Existing application programming interfaces (APIs) should also be preserved in order to add end-to-end security mechanisms at the Transport Layer so that changing existing application programs can be avoided.

2.1.2 Far-Term Requirements

The far-term requirements will likely be met by the *de jure* standard protocols specified by ISO, GOSIP, and IEEE including the Common Management Information Protocol (CMIP) [ISO 90D], File Transfer, Access, and Management Protocol (FTAM) [ISO 88A], Key Management Protocol (KMP), Security Management Protocol (SMP), Generic Upper Layer Security (GULS) Security Exchange Service Element (SESE) [ISO 93B, 93C, 93C, 93D], Connection Oriented Transport Protocol (TP0, TP1, TP2, TP3, and TP4) [ISO 88B], Connectionless Transport Protocol (CLTP), Transport Layer Security Protocol (TLSP) [ISO 94B and 94C], Connectionless Network Protocol (CLNP) [ISO 92B], Network Layer Security Protocol (NLSP) [ISO 94A], X.25 Packet Layer Protocol [ISO 90C], Distributed Queue Dual Bus (DQDB) [IEEE 90], Broadband Integrated Services Digital Network (B-ISDN) [ITU 91], Fiber Distributed Data Interface (FDDI) [ISO 89B, 89C, 90A], Secure Data Exchange Protocol (SDE) [IEEE 93], and others. In addition, other protocols are likely to become international standards. These include Asynchronous Transfer Mode Protocol (ATM) [ITU 91] and Synchronous Optical Network Protocol (SONET) [ANSI 88A, 88B, and 89].

2.2 Interconnectivity and Distributed Processing

Connectivity between classified and unclassified systems and networks must be provided. This connectivity must be capable of networking mainframes, workstations, and PCs in various (dedicated, systems high, multilevel, and compartmented) operational modes. It must provide common security management and be capable of maintaining the identifies of users and information objects under each system or network security policy in order to provide users with access to any information for which they are authorized. A reliable communications architecture must be provided to protect against denial of service, assure timely delivery of information, and provide survivability.

2.2.1 Near-Term Requirements

Interconnectivity must support client-server architectures, distributed processing, and a common security management. Devices that implement security protocols must permit the secure host or subnetwork that they are serving to communicate with other secure components as well as with non-secure components. For example, a secure host that processes classified data must be able to communicate with another secure host that processes classified data, and they must be able to exchange classified information. In addition, the secure host must be able to communicate with a non-secure host that processes only unclassified information, and they must be able to exchange only unclassified information.

Common security management is needed to ensure conveyance of standard information required to manage users, security policies, information and assets, systems and security relevant functions.

Additionally, Naval requirements for interconnectivity include a worldwide Surveillance Grid of sensors and a worldwide Communications Grid of display tools and communications pathways. [CNO 93] The Surveillance Grid concept conceives of sensors operated by various organizations as a grid of capabilities overlaying the battle space instead of a series of single sensors. Software interfaces are used to translate the various sensor outputs into a common binary format, and display tools are used to visualize the sensor output and to monitor perturbations in the grid. The Communications Grid concept conceives of a robust global communications infrastructure consisting of both military and commercial assets. The communications pathways are common and transparent to the grid operators. As with the Surveillance Grid, display tools are used to visualize the communications networks as a grid over the battle space and to route, restore, and task the grid.

Security protocols must function reliably and efficiently under noisy, delayed, and interrupted conditions. For the Naval environment, the communications architecture must ensure EHF low data rate (LDR) SATCOM inherent anti-jam capabilities, anti-jam traffic switching between RF assets, and continual performance while under attack. As technologies for providing high bandwidth become widely available and widely implemented, reliability and survivability of communications architecture will remain an important factor.

2.2.2 Far-Term Requirements

There are no additional requirements identified for the long-term.

2.3 Commercial- and Government-off-the-Shelf Equipment

A primary objective for computer and communications procurements, including information security (INFOSEC) procurements, is the acquisition of COTS/GOTS equipment. There are several reasons for this, including the fact that COTS/GOTS procurements are generally less costly since they minimize the development cost associated with an acquisition. Also, the COTS/GOTS computers and communications products tend to support multiple purposes while specialized products are often designed for a single function. This implies that the products are more likely to be interoperable. In addition, COTS/GOTS implementations generally incorporate state-of-the-art technologies that are flexible and allow for evolutionary porting to new bases.

2.3.1 Near-Term Requirements

External front-end devices that interface between a host computer and the communications system to perform security services are typically specialized products. In line with the goal of procuring COTS/GOTS products, security mechanisms should ideally be implemented in firmware and software that can be installed internally on workstations, yet be afforded comparable access protection to that of external products. In addition, the workstation operating systems must be able to ensure that these internal security mechanisms cannot be bypassed. Implementors must ensure that the new products are interoperable with existing firmware and software.

TEMPEST has long been a security issue for military systems. The solutions have typically been the development of specialized computer and communications equipment which is shielded and filtered to contain emanations, the shielding and filtering of computer facilities, and the assignment of no-entry control zones outside the computer facilities. With the trend toward COTS/GOTS products and mobility, these solutions are no longer acceptable for all environments. However, the achievements in low power consumption have greatly reduced the level of emanations that are emitted from computers. TEMPEST considerations will continue to require some shielding and filtering and will necessarily restrict the mobility of users desiring to access highly sensitive data until new solutions can be found. However, there is also a trend toward relaxation of the TEMPEST requirements.

2.3.2 Far-Term Requirements

Encryption devices for classified communications traffic may be developed commercially and provided off-the-shelf in the long-term.

2.4 Processing Speed

Transmission rates have in the past been in the range of 10 Kbps to 10 Mbps. Multimedia applications are imposing requirements in excess of 30 Mbps for individual workstations connected to Naval LANs. Fiber optic media and protocols are bringing LAN, MAN, and WAN speeds of 100 Mbps to 2.5 Gbps, with an outlook of 50 Gbps within a few years.

2.4.1 Near-Term Requirements

Security products must function at extremely high speeds and provide new services to keep up with evolving technology. Performance constraints may preclude use of encryption in these systems. Alternate confidentiality mechanisms such as protected distribution systems and protected fiber techniques may be needed.

2.4.2 Far-Term Requirements

There is an ever increasing demand for more bandwidth, which shows no bound. Therefore, there will be ever increasing far-term security implementation requirements.

2.5 Multilevel Secure Connectivity

Multilevel secure processing and communications must be provided to ensure that systems containing information with different sensitivities and users with different security clearances and need-to-know levels allow simultaneous access to permitted information while preventing users from accessing information for which they lack authorization.

2.5.1 Near-Term Requirements

Multilevel secure connectivity depends on the development of standards, protocols, and interfaces that define a cohesive multilevel security architecture. Evolutionary and affordable security solutions for meeting information systems multilevel security needs must be provided.

2.5.2 Far-Term Requirements

Secure and interoperable COTS/GOTS software and firmware must be developed and fielded for the approaching multilevel multimedia environments.

2.6 Secure User Mobility

User mobility introduces security implementation requirements that were not present for stationary environments.

2.6.1 Near-Term Requirements

When authorized, users must be able to log-on to their system from any workstation in the network. Eventually this may imply access from nearly *any* workstation in the world since most workstations will be networked. The security issues include providing authentication and access control for these users. Mobility concerns also include the ability for computers to interface to the network through cellular telephone and to retain connectivity as they move from one location to another. The implication is that as users change domains, the addresses associated with their connections must be updated throughout the network so that messages will continue to be delivered correctly. Another mobility issue is concerned with wireless LAN technology. This is conceived of as a limited line-of-sight communications capability that allows computers to move around a ship or repair facility without having to be physically connected to LAN cables. Concerns include interference with transmissions and ensuring the timely delivery of traffic.

With mobility comes an emphasis on the need for small computer products. Support products, such as communications and security products, must also be as small as possible. This emphasizes the need to install these products internally, in firmware where necessary, and in software where possible. Similarly, mobility causes a requirement for reducing power usage. Side benefits include lower heat output and less signal emissions.

2.6.2 Far-Term Requirements

There are no additional requirements identified for the long-term.

2.7 Secure Multimedia Communications

Automation is moving toward integrated services digital networks (ISDNs) which provide voice and non-data communications concurrently, and later toward broadband ISDNs (B-ISDNs) which will provide even greater bandwidths to support any type and mix of traffic. Multiple signals will be relayed by Asynchronous Transfer Mode (ATM) over the same channel via isochronous time slots, called *cells,* that are not preassigned, but are available upon demand. Various adaptation layers will overlay ATM to deliver a constant voice rate, a high speed variable data rate, or other service as needed.

2.7.1 Near-Term Requirements

Security must be implemented during the development of the devices that will provide ISDN and B-ISDN switching and signaling to ensure that transmissions are not lost, delayed, corrupted, or compromised. Secure display (windows) implementations are needed for integrated multimedia (voice, data, whiteboarding, imagery, and video). Standards bodies are addressing these issues so that protocols, mechanisms, and the products that implement the protocols and mechanisms will function as intended.

2.7.2 Far-Term Requirements

As users become comfortable with the new capabilities provided by B-ISDN, there will be a demand for additional capabilities. New technologies that arise out of this demand must also be designed to achieve security.

2.8 Security Firewalls

A firewall has been defined as [CHES 94]:

> *A collection of components placed between two networks that collectively have the following properties:*
>
> - *All traffic from inside to outside, and vice-versa, must pass through the firewall.*
> - *Only authorized traffic, as defined by the local security policy, will be allowed to pass.*
> - *The firewall itself is immune to penetration.*

Firewalls must be incorporated in order to protect each subnetwork or system against intrusion. The firewall is a secure front-end or secure relay (i.e., bridge, router, and protocol converter) that prevents unauthorized users from accessing computing resources on the system or network, and unauthorized and unnoticed export of information.

2.8.1 Near-Term Requirements

Guard technology can be implemented to provide firewall security in the form of secure front-ends and secure relays between subnetworks. The network guards should be capable of implementing both identity-based (discretionary) and rule-based (mandatory) access control policies.

2.8.2 Far-Term Requirements

In light of the fact that users are becoming mobile and that network components occasionally fail or are moved, networks must be reconfigurable to allow the state of the relays and their associated ports to be dynamically changed. Care must be taken to develop algorithms that authenticate configuration messages so that an adversary could not corrupt the network by transmitting spurious information. In addition, firewalls must not reveal information which could be used to infer sensitive or classified information about hosts on the secure side to hosts on the non-secure side. Specific far-term requirements for secure relays have not yet been developed.

2.9 Selectable Security Services

The following security services must be provided for the Naval environment so that system implementors can select those needed for their specific mission:

- Authentication verifies the identity of a user or device in order to counter the threats of masquerading or playback
- Access control of information, services, and equipment prevents any unauthorized use of a resource or use of a resource in an unauthorized access mode. Mandatory access control is enforced through the use of security labels associated with each service data unit exchanged and with all network entities. These security labels must be protected by use of label binding or integrity mechanisms
- Confidentiality of user and system information protects against unauthorized disclosure and minimizes the threat of eavesdropping
- Integrity of information, software, and equipment ensures that only authorized changes to data, information, or processes occur and thus minimizes the threat of unauthorized modification
- Non-repudiation protects against the originator or recipient of a message from denying origination or receipt. Non-repudiation is provided as either proof-of-origin or proof-of-delivery, or both
- Traffic flow confidentiality may be needed to ensure that interconnected systems do not reveal too much information about users and their mission, particularly when a network link traverses unprotected portions of the network and protocol control information may be needed by relays in those areas.

2.9.1 Near-Term Requirements

The security services (authentication, access control, confidentiality, integrity, and non-repudiation) must be provided on a node-to-node-basis as well as a user-to-user basis. In addition to these security services, auditing, and dynamic key management must also be provided. Audit trails support traceability and individual accountability of users and devices. Dynamic key management ensures that key generation, distribution, storage, and updating occurs in a secure manner.

2.9.2 Far-Term Requirements

The same security services (including audit and dynamic key management) will be required when future technology becomes available.

2.10 Secure Multicast Routing

Multicast, a method for delivery of message traffic to multiple receivers, is being addressed in communications protocols by both Internet and international standards bodies. The Internet Engineering Task Force (IETF) has developed three protocols (Distance-Vector Multicast Routing Protocol, Protocol-Independent Multicast Routing Protocol, and Multicast Open Shortest Path First Routing Protocol) and is in the process of developing a fourth (Core-Based Trees Routing Protocol). ISO standards bodies have similar efforts underway. No single protocol has emerged as the clearly superior product.

Multicast implementations require that the source host transmit as few copies of a message as possible and that relay systems located near the recipients burst the message into multiple copies for final delivery. For example, if a sender located in San Francisco wishes to transmit a message to five recipients who are all located in New York, multicast would cause one message to be transmitted through the network to a relay in New York which in turn delivers the message to all five recipients. If some groups of recipients are located on different subnetworks, it may be necessary for an intermediate relay to create multiple copies that are forwarded to other relays which in turn create multiple copies for final delivery to each recipient in their group.

2.10.1 Near-Term Requirements

Security must be considered during the development of multicast protocols and multicast extensions to existing communications protocols. The protocols must be developed in a manner that ensure messages will be delivered efficiently to all intended recipients (service assurance) and no others (access control).

Multicast extensions must also be compatible with security protocols that perform confidentiality and integrity services. The location of a security protocol entity may have an impact on the multicast implementation. For example, if a protocol entity is located

at a secure relay rather than in the end system, relocation of the end system will require that the multicast algorithms that track host locations to also coordinate with the security protocol entity to confirm that delivery will be permissible at the new location. Consideration must also address whether security associations must be established individually between each of the pairs in the cryptonet (multicast group) or must be established jointly for the entire group.

2.10.2 Far-Term Requirements

The secure relays that will perform multicast services in a multilevel environment must be aware of rule-based and identity-based security characteristics of the recipients and must make access control decisions based on those characteristics prior to transmission. In addition, relays must not reveal information which could be used to infer sensitive or classified information about hosts to unauthorized entities. Specific far-term security implementation requirements for multicast routing capabilities have not yet been developed.

Section 3

Characteristics of Current Environments

This Page Intentionally Left Blank

3.0 Characteristics of Current Environments

Existing and in-design security products were compared with the proposed network security requirements in order to evaluate the current environment. The purpose of this study was not to produce an in-depth product analysis, but to identify security requirement areas that may not be adequately addressed by current technology. Therefore, the analysis did not review the security products in depth nor determine to what degree they fulfilled each requirement.

The security implementation requirements discussed in Section 2 are summarized in Table 3-1 below. Section 3.1 describes briefly the functionality and security properties of some network security products that may satisfy some of those requirements. The MISSI product descriptions are particularly terse since they are well documented elsewhere. Both Type 1 and Type 2 network security products that are implemented in workstations were reviewed. However, only Type 1 LAN and WAN interface products were reviewed. The network security products are categorized as follows:

- Workstation Products and Peripherals for Type 2 (Sensitive but Unclassified) Processing
- Workstation Products and Peripherals for Type 1 (Classified) Processing
- Type 1 Local Area Network (LAN) Interface Products
- Type 1 Wide Area Network (WAN) Interface Products.

Because open systems interconnection is a major requirement for networking, protocol suites are discussed briefly in Section 3.2. These include DoD (i.e., TCP/IP), International Standards Organization (ISO), and security protocol suites. Section 3.3 discusses the security posture of the Naval information processing environment.

3.1 Network Security Products

Both Type 2 and Type 1 security products, existing and in research and development, were reviewed to determine whether they appeared to meet the Naval security requirements described in Section 2. Some of the products which exist only as research projects may never actually become available products. All of the Type 2 products are either workstation peripherals, or software that runs on a workstation. These include the Clipper and Capstone chips, MISSI MOSAIC workstation peripheral, Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP) encryption algorithm, Kerberos, and Krypto-Knight.

Type 1 workstation products that were reviewed include the MISSI Crypto-Peripheral, MISSI Appliqué, ITT Dragonfly, NCCOSC RDTE DIV (NRaD) All Purpose Workstation Security Peripheral (ALLPOWER) [NRaD 92 and 94B], Naval Research Laboratory (NRL) Embeddable INFOSEC Product (EIP) [SPAWAR 92B], and Message

Table 3-1. Requirements Summary

1. Secure Open Systems Architecture
   - Open system standards
     - DoD / Internet (TCP, IP, SMTP, FTP, Telnet, SNMP)
     - ISO (COTP, CLNP, X.400, X.500, CMIP)
     - Security (SDNS MSP, SILS, NLSP, TLSP)
   - Preserve existing APIs
2. Interconnectivity and Distributed Processing
   - Interface in all operational security modes
   - Connectivity between classified and unclassified
   - Connectivity between secure and non-secure systems
   - Support distributed client-server architecture
   - Maintain user and object IDs by security policy
   - Common security management
   - Reliability and survivability
3. Maximize use of COTS/GOTS Hardware and Software
4. Security Processing at Extremely High Speeds
5. Standards, Protocols, and Interfaces for Multilevel Security
6. Secure User Mobility
   - Allow users to have access from anywhere in network
   - Address mobility across subnetworks
   - Secure wireless technology
7. Secure Multimedia Communications
8. Secure Firewalls
   - Front-ends
   - Relays
9. Selectable Security Services
   - Identification and Authentication
   - Access controls
   - Confidentiality
   - Integrity
   - Non-repudiation
   - Labeling
   - Auditing
   - Dynamic key management
10. Secure Multicast Routing

Security Protocol (MSP) devices. Secure workstations, such as the Compartmented Mode Workstation (CMW) and the Trusted Information Systems T-MACH, were not reviewed. Security products designed for a workstation must be used in conjunction with a trusted workstation in order to provide assurance that the information delivered by the workstation to the security peripheral has maintained its integrity and is authentic.

Type 1 LAN products that were reviewed include the GTE Tactical End-to-End Encryption Device (TEED), Wang Trusted Interface Unit (TIU), Verdix Secure LAN, Boeing MLS LAN, Xerox Encryption Unit (XEU) and Xerox Ethernet Tunnel (XET), MISSI Network Security Manager (NSM), and the MISSI Secure Network Server (SNS) Fileserver. Type 1 WAN products being reviewed include SNS Guard/Regrader, Radiant Mercury, MISSI In-line Network Encryptor (INE), and Synchronous Optical Network (SONET) and Asynchronous Transfer Mode (ATM) encryptors.

3.1.1 Workstation Products and Peripherals – Type 2

Six Type 2 products for user workstations were reviewed. As mentioned earlier, they are the Clipper and Capstone chips, MISSI MOSAIC workstation peripheral, Privacy Enhanced Mail, Pretty Good Privacy encryption algorithm, Kerberos, and Krypto-Knight.

Clipper and Capstone Chips. Clipper and Capstone are a family of chips that implement the Skipjack algorithm (a replacement for DES) [SKIPJACK 93] [CLIPPER 93] for protecting Types 2 and 3 data. Clipper chips provide confidentiality through symmetric encryption. Capstone chips provide data origin authentication (through digital signatures), data integrity (through use of the secure hash algorithm), non-repudiation, and key management. Clipper and Capstone chips are installed on FORTEZZA (formerly 'TESSERA') crypto-cards which a user inserts into the workstation PCMCIA peripheral. Current implementations include DOS, Windows, UNIX, Macintosh, and AT&T 3B2 platforms.

While DES uses a 56 bit Traffic Encryption Key (TEK), Skipjack uses an 80 bit TEK to provide additional strength. The Skipjack algorithm (and thus the Clipper and Capstone Chips) is a key-escrow system. It includes a Law Enforcement Access Field (LEAF) which allows a third party (presumably law enforcement) to use an Escrow Key to determine the TEK in order to eavesdrop. However, the Escrow Key is split into two half-keys which are held by separate government agencies acting as escrow agents. In addition, a Family Key, which is held by a third agency, is needed to identify the serial number of the escrow device so that the correct escrow half-keys can be obtained from the two escrow agents. Therefore, the Family Key and both halves of the Escrow Key are needed in order to use the LEAF to allow electronic surveillance.

Users are allowed to logon to the network from any terminal that is equipped with a "smart card" peripheral device that supports these chips. Users can communicate with other users who are located at non-equipped workstations in a non-secure mode.

Clipper and Capstone are not intended for use with classified data and as such will not support multilevel secure (MLS) processing.

Early testing indicates processing rates of the Clipper and Capstone chips of up 12 Mbps. The chips are designed to support dynamic key management on a session basis. They also support multicast routing of traffic. Failure of the chips or peripheral on a particular host could prevent the delivery, or secure delivery, of traffic from and to that host.

MISSI MOSAIC Workstation Peripheral. MOSAIC [NSA 93B and 94] is implemented as a workstation peripheral which provides writer-to-reader security services for Unclassified but Sensitive electronic mail (e.g., SMTP or X.400), file transfer (e.g., FTP or FTAM), and other electronic messaging applications. MOSAIC works with the Clipper and Capstone Chips, which implement the Skipjack algorithm and have a LEAF, to perform digital signature (using the Digital Signature Algorithm) and secure hashing (using the Secure Hashing Algorithm). MOSAIC users insert FORTEZZA Crypto Cards, which contain the Clipper and Capstone chips and the user's cryptographic data and which perform all cryptographic functions, into the PCMCIA device. MOSAIC will process traffic at approximately the rates that the Clipper and Capstone chips perform hashing and encryption.

MOSAIC, formerly called *"Preliminary Message Security Protocol (PMSP),"* is a version of the Secure Data Network System (SDNS) Security Protocol 7 (Message Security Protocol) that has been adapted for the Defense Message System (DMS) for use over either a TCP/IP network or the X.400 Message Handling System (MHS). MOSAIC is designed to interface with most hardware platforms, operating systems, applications, network configurations, and communications protocols for open systems interconnectivity. Applications that follow Application Programming Interface (API) specifications do not have to be modified because the MOSAIC security protocol interfaces with the application through the API.

MOSAIC services include data origin authentication (through public-key digital signatures), Type 2 encryption (through symmetric cryptography), data integrity (through use of a public-key one-way hash algorithm), non-repudiation with respect to origin and destination (also based on digital signatures), and electronic key management.

MOSAIC supports dynamic key management. The originator generates a symmetric Traffic Encryption Key (TEK) and encapsulates it using a two-step public-key cryptography approach. First, the TEK is signed for authentication purposes using the originators private key, then it is encrypted again using the recipients public key for confidentiality. Public keys are bound to user identities through the use of certificates issued by a Certification Authority. With regard to MLS, MOSAIC is designed to protect only Sensitive but Unclassified traffic.

MOSAIC also support multicast routing. A user wishing to send a message to a group of recipients will send the message to a Mail List Agent, which performs the same cryptographic functions on the message that a MOSAIC User Agent would perform and mails the message to each of the recipients.

Failure of the MOSAIC device connected to a particular workstation could prevent the secure delivery of traffic from and to that workstation. While failure of MOSAIC could cause denial of service at the one host, its failure would not significantly affect the operations of the overall system.

Privacy Enhanced Mail and Pretty Good Privacy. Two commercially-developed protocols are being implemented to provide security for electronic mail. Neither contains NSA approved Type 1 encryption and are, therefore, limited to processing unclassified information. They are:

- Privacy-Enhanced Electronic Mail (PEM) [RFC 93B]
- Pretty Good Privacy (PGP) [ZIMMER 92]

PEM is the Internet standard for providing data origin authentication, data confidentiality, data integrity, non-repudiation of origin, and key management for electronic mail messages transmitted using the Simple Mail Transfer Protocol (SMTP). As with nearly all encryption based protocols, PEM uses symmetric encipherment (DES, though other algorithms may be used in the future) for data confidentiality. That is also the basis for the non-repudiation service with respect to origin. PEM uses either MD2 or MD5 to provide a Message Integrity Check (MIC) for data integrity. For authentication and key management, PEM allows the use of either a symmetric approach using DES or an asymmetric approach using RSA public-key encipherment and X.509 certificates. PEM can be installed on a user-by-user basis or site-by-site basis. PEM is non-invasive with respect to the message transfer system. This facilitates its selective deployment at end systems and its selective use by users, thus allowing PEM stations to communicate with non-PEM stations. Of course, such communications would not be secure.

PGP is a public-domain encryption program that is considered by some to be *"the closest you're likely to get to military-grade encryption."* [SCHNEIER 94] PGP provides authentication, data confidentiality, data integrity, and key management for electronic mail, principally SMTP. PGP uses MD5 as a one-way hash function for authentication and data integrity. Instead of using DES for data confidentiality, PGP uses another symmetric algorithm called the International Data Encryption Algorithm (IDEA). IDEA follows ANSI X9.17 to generated random keys. Signatures, when included, are encrypted with the message text for confidentiality. PGP does not use certificates. Users distribute their own public keys. PGP also compresses files before encryption. Both PEM and PGP support multicast by using asymmetric encryption to transmit the TEK to each intended recipient.

Two well known implementations of PEM for use with SMTP are TIS-PEM, developed by Trusted Information Systems to run on most Unix hosts, and RI-PEM, developed by Mark Riorden and controlled by Public Key Partners. Both use RSA for key management. PGP is public domain software which is available over the Internet and is being used extensively with SMTP.

The PEM products are well-tested software based applications that have been installed on a wide variety of Unix hosts. PEM and PGP are not interoperable with each

other or other mail privacy applications. Therefore, failure of these algorithms on a particular host could prevent the secure delivery of mail traffic from and to that host. While failure of the product could cause denial of service of mail traffic at that station, their failure would not significantly affect the operations of the overall system. The throughput rate for either PEM or PGP is essentially the rate that a particular processor processes the DES Data Encryption Algorithm. Beyond that, PEM and PGP do not incur significant overhead.

PEM supports dynamic key management. The originator generates a symmetric Traffic Encryption Key, encapsulates it using either symmetric or asymmetric encipherment, and transmits it to the authorized recipients to enable them to recover the original message. When an asymmetric encipherment approach is used, public keys are bound to user identities through the use of certificates issued by a Certification Authority. PGP also allows dynamic key management with symmetric TEKs being encapsulated via asymmetric encipherment for distribution. However, PGP does not employ certificates for the authentication of public keys.

Kerberos and Krypto-Knight. The Kerberos Authentication System is a dynamic key distribution system with user authentication. Kerberos is designed for a client-server environment to provide unforgeable credentials that identify individual users to servers. Each principal (user or server) shares a private key with the Kerberos Key Distribution Center (KDC). This key is used to distribute a TEK and an authenticator (a certificate of authenticity) to the principal. Authentication is provided by virtue of the fact that the Kerberos KDC is a trusted third party and that only the KDC and the principal share the private key. The principal will use the TEK to communicate with the server that receives the matching TEK.

To ensure integrity, all Kerberos messages contain a checksum. To prevent replay, four of the five messages required for the exchange include the user's IP address and a timestamp. However, the first message (which is a request sent by the user to the KDC to begin the authentication exchange and obtain a server session key) contains no authentication information and, in fact, is not encrypted. Also, since the reply message is encrypted using a one-way hash of the user's password, there is a risk that a determined adversary that intercepts the encrypted reply message from the KDC could determine the password using a brute force password guessing attack off-line. If the attack is successful and is accomplished before the session key expires, the adversary would acquire the information needed to acquire the session key. [SCHNEIER 94]

Another limitation of Kerberos is that it is designed for user-to-host authentication, not host-to-host authentication. It is useful for users to authenticate themselves prior to gaining access to servers. However, hosts that use Kerberos to access other hosts for services such as mounting remote file systems are vulnerable because they would have to maintain keys for themselves without allowing the keys to be compromised. Hosts are not known for their ability to keep secrets for long periods. [CHES 94]

Krypto-Knight is an authentication and dynamic key distribution system developed by IBM which is similar to Kerberos, though not as widely implemented. It uses private key techniques, as does Kerberos. It provides three authentication services: user authentication (called Single Sign-On), two-party authentication, and data origin authentication. [SCHNEIER 94]

3.1.2 Workstation Products and Peripherals – Type 1

Six Type 1 products for user workstations were reviewed. As mentioned earlier, they are the MISSI Crypto-Peripheral, MISSI Appliqué, ITT Dragonfly, NRaD All Purpose Workstation Security Peripheral (ALLPOWER), NRL Embeddable INFOSEC Product (EIP), and Message Security Protocol (MSP) devices.

MISSI Crypto-Peripheral. The Crypto-Peripheral (CP) is an upgrade to MOSAIC. CP uses a PCMCIA smart-card peripheral and incorporates a Type 1 algorithm to provide single-classification security for Unclassified through Secret electronic mail.

MISSI Appliqué. Appliqué consists of hardware and software that will be added to a secure operating system (TMach) to provide Unclassified through Secret multilevel security internally within the trusted workstation. In addition to supporting electronic mail, Appliqué will provide MLS services for file transfers.

Appliqué provides user identification and authentication based on personal identification number (PIN) and userid, host-level identity-based access control (IBAC) based on Network Layer source ID, rule based access control based on Commercial Internet Protocol Security Option (CIPSO) and KMP labeling, peer entity authentication (using NLSP), data origin authentication (using MSP or NLSP), confidentiality (using MSP or NLSP), non-repudiation, and audit.

ITT Dragonfly. Dragonfly is intended to be a product that will interface with Appliqué and provide the means for protecting MLS communications over untrusted networks. Dragonfly security services will include electronic key management and data origin authentication for connectionless communications. It will be designed to meet B2 criteria for processing two adjacent levels of data (i.e., Sensitive but Unclassified and Confidential, Confidential and Secret, etc.).

All Purpose Workstation Security Peripheral (ALLPOWER). ALLPOWER, being proposed by NRaD [NRaD 92 and 94B], will be a Compartmented Mode Workstation (CMW) peripheral security device designed to provide multilevel operations and multimedia access of shipboard systems connected to the Communications Support System (CSS) shared communications environment. It is in the concept phase, and may possibly never be developed. However, it has a unique and interesting approach.

ALLPOWER will support both multilevel and single-level workstations, servers, and LANs. It will provide Application Layer service in order to provide security to the granularity of the individual user or process. Since ALLPOWER will provide Application

Layer service, it will not be tied to any particular communications protocols. The ALLPOWER will use interchangeable cards for flexibility to interface with existing and future Transport Layer communications protocols (e.g., TP4, TP1, TCP, UDP).

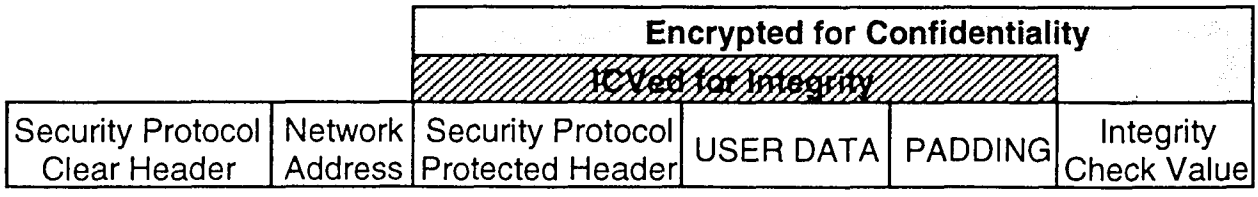
Security services that will be provided include peer-entity authentication (through digital signatures), data confidentiality (through Type 1 encryption), sensitivity labeling, mandatory and discretionary access control, non-repudiation, and audit (maintained by the host operating system).

Users will be required to insert an identification card into the ALLPOWER unit and enter a password in order to logon to the workstation. User identities will be bound to the identification card holding individual keying material. What is unique about this device is that the user can work from any ALLPOWER-equipped workstation in order to facilitate user mobility.

An MLS network manager will create user accounts, assign privileges, write keys to user identification cards, and distribute the cards to the users. The manager will also collect and review audit data at an MLS Manager workstation. The ALLPOWER will use BLACKSIDE Over-the-Air-Rekeying (OTAR) for dynamic key management. The devices will not require that a user identification card be inserted for keying.

Embeddable INFOSEC Product (EIP). The EIP [SPAWAR 92B], being developed by NRL, will be a workstation peripheral designed to provide Type 1 security services at the Transport Layer or the top of the Network Layer. It is also in the research and design phase. As shown in Figure 3-1, the EIP will be interoperable with any Transport and Network Layer communications protocols, but will not include those protocols itself. The EIP will include standard security protocols (e.g., TLSP, NLSP, SP4, SP3). This will enable the EIP to interface with any existing or future protocol stack without modification. Security services planned to be supported by the EIP include data confidentiality, data integrity, authentication (supporting access control), labeling, and traffic flow confidentiality. It will employ out-of-band key management consistent with the Navy Key Distribution System (NKDS).

The EIP will apply a cryptographic checksum to the Security Protocol Protected Header, user data, and padding field for integrity, as shown below. The EIP will encrypt those fields, as well as the ICV, for confidentiality. The clear header (including address information) will bypass the integrity and confidentiality processing functions and be passed unprotected between the domains. Control PDUs may also bypass protection and be passed in their entirety.



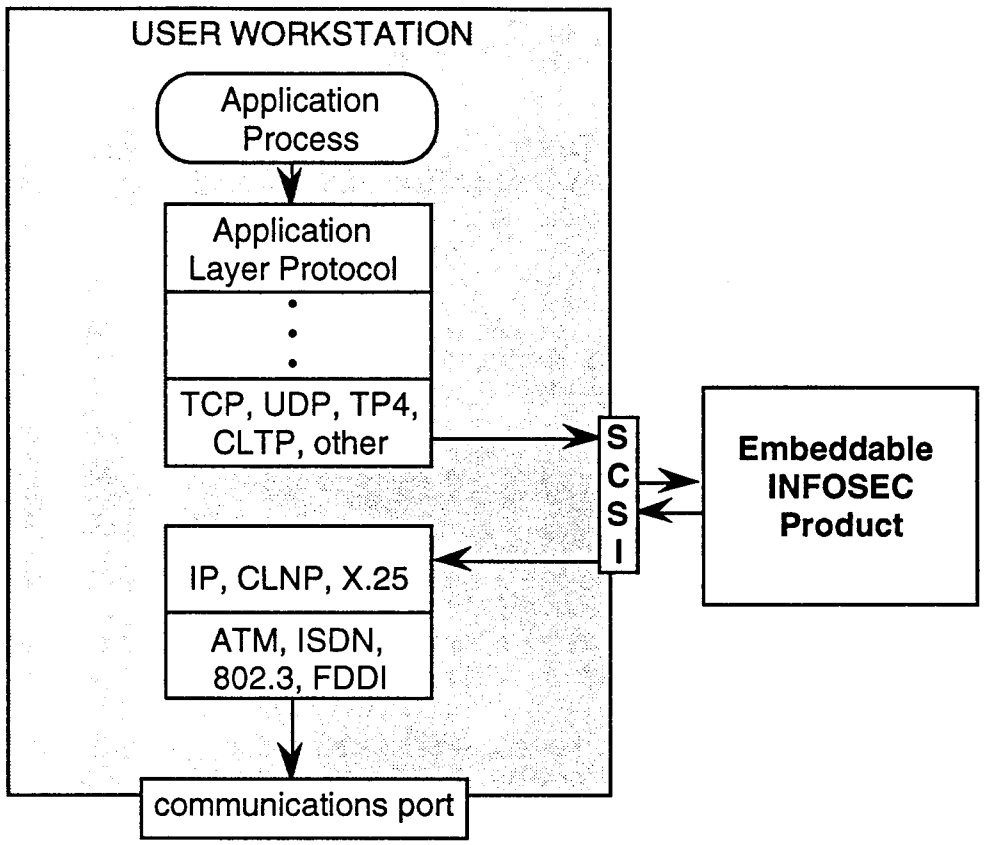


Figure 3-1. Embeddable INFOSEC Product Functionality

Messaged Security Protocol (MSP) devices. The SDNS Security Protocol 7, called the Message Security Protocol (MSP), is intended to protect Type 1 X.400 message traffic. MSP provides writer-to-reader confidentiality, integrity, data origin authentication, non-repudiation with proof of origin, request for a signed receipt of delivery (though there is no guarantee that a receipt will be returned), and access control during message transfer. [NIST 93]

The MSP can be implemented internally in software within a trusted workstation, or in a peripheral device. If internal placement is selected, MSP may have a substantial impact on throughput because it would require CPU time in order to perform its services. Therefore, it would be preferable to implement MSP on a separate processor. Since it is implemented at the Application Layer, it would not be appropriate to implement it in a front-end device. The MSP supports multiple addressees and is suitable for multicast routing by a routing protocol.

3.1.3 LAN Products – Type 1

Type 1 LAN products that were reviewed include the GTE Tactical End-to-End Encryption Device (TEED), Wang Trusted Interface Unit (TIU), Verdix Secure LAN, Boeing MLS LAN, Xerox Encryption Unit (XEU) and Xerox Ethernet Tunnel (XET), MISSI Network Security Manager (NSM), and the MISSI Secure Network Server (SNS) Fileserver.

Tactical End-to-End Encryption Device (TEED). The GTE Tactical End-to-End Encryption Device (TEED) is a host front-end communications device that is inserted between a workstation and an IEEE 802.3 LAN or X.25 packet network to protect data on the LAN. The TEED provides end-to-end Type 1 encryption/decryption and authentication. The TEED is ruggedized and TEMPEST-approved and is suitable for use in tactical environments.

Each user selects the security level they want the TEED to operate at for each session. Levels specified may be Unclassified, Secret, Top Secret, or TS/SCI. The TEED can operate at multiple security levels when attached to a trusted host computer that implements the IP Security Option to add security labels to IP PDUs.

The TEED can use traditional key fill. In this case, operational keying material is provided manually via a key storage device. In addition, TEED can use Firefly dynamic rekeying to perform electronic key exchanges with the SDNS electronic key management system (EKMS) over the black network and generate traffic encryption keys (TEKs) for the communications session between two parties.

Trusted Interface Unit (TIU). The Wang Trusted Interface Unit (TIU) is a stand-alone communications device that is inserted between a workstation or a cluster of workstations and an Ethernet LAN. It performs Type 1 encryption through TS/SCI by implementing proprietary security functionality at the Data Link Layer. It provides single-classification secure communications over a non-secure LAN which can be used simultaneously to carry unclassified traffic. The TIU is able to generate IP headers in order to route the PDU through an internetwork. Multicast and broadcast messaging is supported. The TIU has a throughput rate of 2.4 Mbps (based on 200 1,500-byte frames per second).

The Network Security Officer (NSO) assigns users and TIUs to a specific group and security level. Users are required to physically insert a Crypto Ignition Key (CIK) into the TIU to activate the device. The CIK must be preloaded with the TEK by the NSO. Users may communicate with other individuals or with groups of individuals when all users in the group share the same TEK. Multiple CIKs may be inserted simultaneously into the TIU to allow communications to multiple destinations under different TEKs. Key distribution is performed manually. Dynamic key management is not supported.

Verdix Secure LAN. The VSLAN, consisting of a Network Security Center (NSC) and up to 128 Network Security Devices (NSDs) as shown in Figure 3-2, provides multilevel secure communications (for two adjacent classification levels) on a standard Ethernet LAN. The Ethernet backbone can be shared by stations that are not secured by VSLAN. However, secure stations cannot communicate with non-secure stations. The NSD is a trusted network interface board that plugs into a variety of computer backplanes. The VSLAN has been certified at the B2 level of trust. Several VSLANs can be internetworked using a Verdix Secure Internet Protocol router (VSIP). The VSIP also allows single-level LANs to be connected to multilevel (i.e., two level) LANs. Secure communications can be provided to remote terminals by interfacing a Verdix Network Terminal Server to the VSIP using X.25. Security services include user identification and authentication (I&A), Type 2 (DES) encryption (not usable for providing confidentiality for classified information), integrity, mandatory and discretionary access control, and auditing.

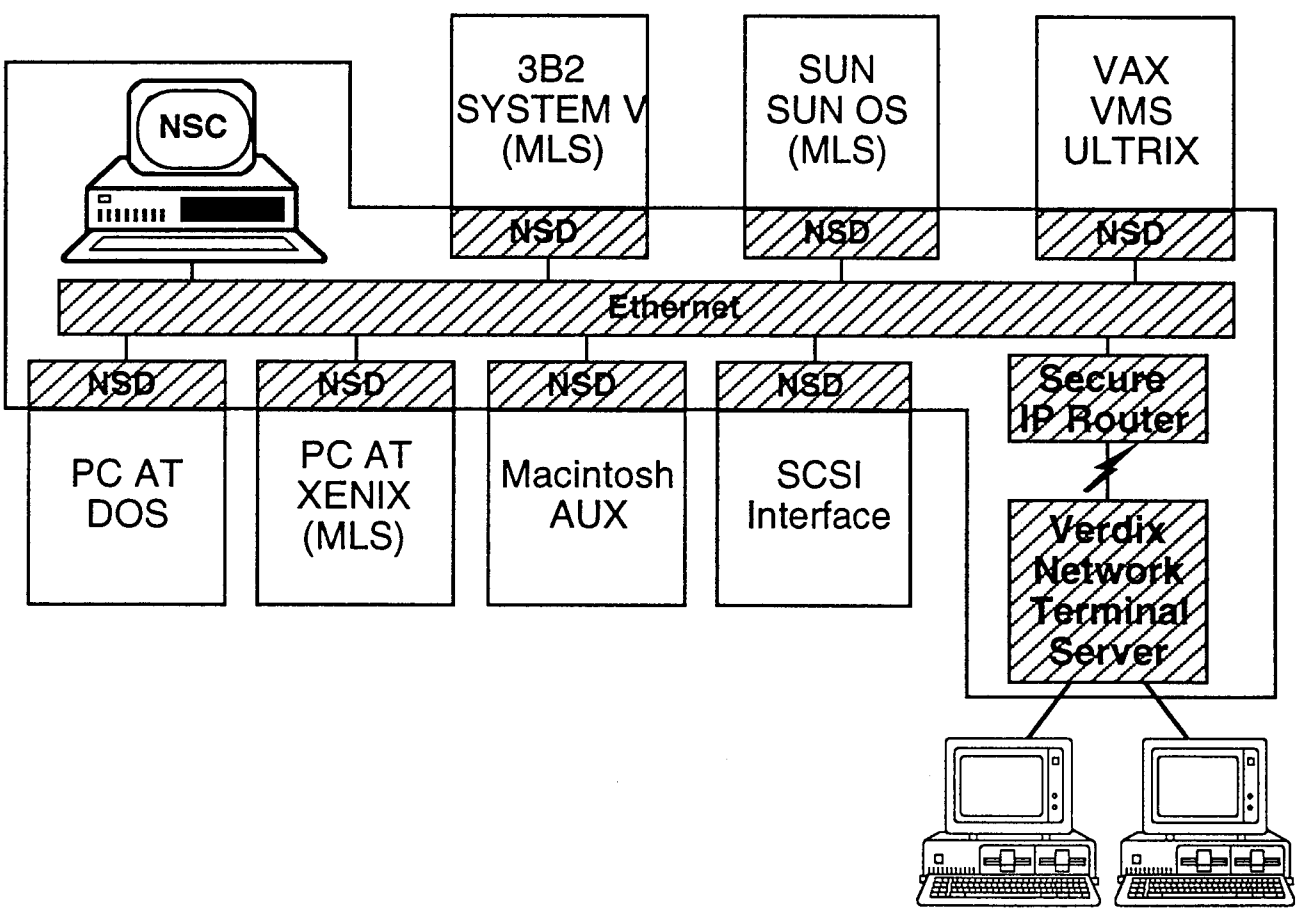


Figure 3-2. Verdix Secure LAN Configuration

As with other workstation products, I&A is done with something the user possesses -- a Datakey. The user identity is bound to the Datakey. In order to logon to a terminal, the user physically insert the Datakey into the NSD. If the user inserts the key into an unauthorized NSD, the key is rendered invalid. Audit entries are generated by both NSDs and the NSC, but are journaled only at the NSC. Audit granularity is to the host level and not to the single user level because the NSD is not aware of host operating system events or user processes. However, the NSC is able to audit network events to the level of the user associated with the Datakey.

Integrity is provided through encryption. The NSD and NSC change their keys each time they communicate. Traffic Encryption Keys are provided electronically by the NSC and are changed periodically, through dynamic key management. However, they are not typically issued for each session. (With another product, the VSLAN II, designed for Type 2 confidentiality, message authentication codes can be generated to provide data integrity, and sequence numbers can be included to support connection integrity.)

Mandatory Access Control ranges are established by the security policy and defined by the NSO working at the NSC. The NSC assigns the range of classification levels and categories that may be processed by each NSD. Minimum and maximum classification levels and categories are granted separately for transmit and receive. The user selects the session level during logon. The NSD then enforces the mandatory access control policy. The VSLAN affixes sensitivity labels to Ethernet frames and mediates all LAN data transfers to ensure they are within allowable Mandatory Access Control ranges.

The NSO also establishes two forms of Discretionary Access Control (DAC): first, the NSO defines which users are allowed to gain access to individual NSDs, and second, the NSO defines which NSDs can communicate with each other. Again, transmit and receive permissions are granted separately. The VSLAN then mediates data transfers with regard to DAC definitions.

The security policy may specify that a group of users be issued the same TEK so that traffic can be multicast to all users in the group. The NSD Datakey reader supports up to 100 policies. Therefore, a user could use a group key to communicate with some users and could use a different key to communicate with other users.

Throughput rates for VSLAN with all traffic being encrypted is approximately 2.3 to 2.8 Mbps. When only authentication is performed, the throughput increases to approximately 5.5 Mbps. A modification to the hardware currently under B2 RAMP evaluation will boost speeds by 20 to 30 percent. The vendor plans to support high speed Ethernet next year when it is standardized. Verdix claims that VSLAN processing will be in the neighborhood of 80 to 90 Mbps.

Boeing MLS LAN. The Boeing MLS LAN is based on a stand-alone communications device certified at the A1 level, called the Secure Network Server (SNS), that is inserted between a workstation and a LAN to provide identification and authentication, labeling of

PDUs, mandatory and discretionary access control, audit, and traffic flow confidentiality (provided by data padding). The SNS does not provide a data confidentiality service. It interfaces both single-level and multilevel hosts to an Ethernet or FDDI (future) LAN. In addition to digital data transmission, the SNS supports simultaneous transmission of analog video signals. The network security administrator interfaces to the network through an SNS that is augmented with a Network Management Module (NMM). The security administrator assigns the range of classification levels that may be processed by each SNS. The SNS enforces the mandatory access control policy.

Like the VSLAN, MLS LAN audit entries are generated by both SNSs and the NMM, but are journaled only at the NMM. Audit granularity is to the host level and not to the single user level because the SNS is not aware of host operating system events or user processes. The host must be relied upon to audit user activity. Similarly, the host must be relied upon to properly label frames submitted to the SNS for validation and transmission.

The SNS implements TCP, IP, UDP, and Telnet protocols and provides security services at or above the Transport Layer. Future versions will include ISO protocols. MLS LAN throughput between workstations is approximately 235 Kbps. Boeing is targeting 1 Mbps for future versions.

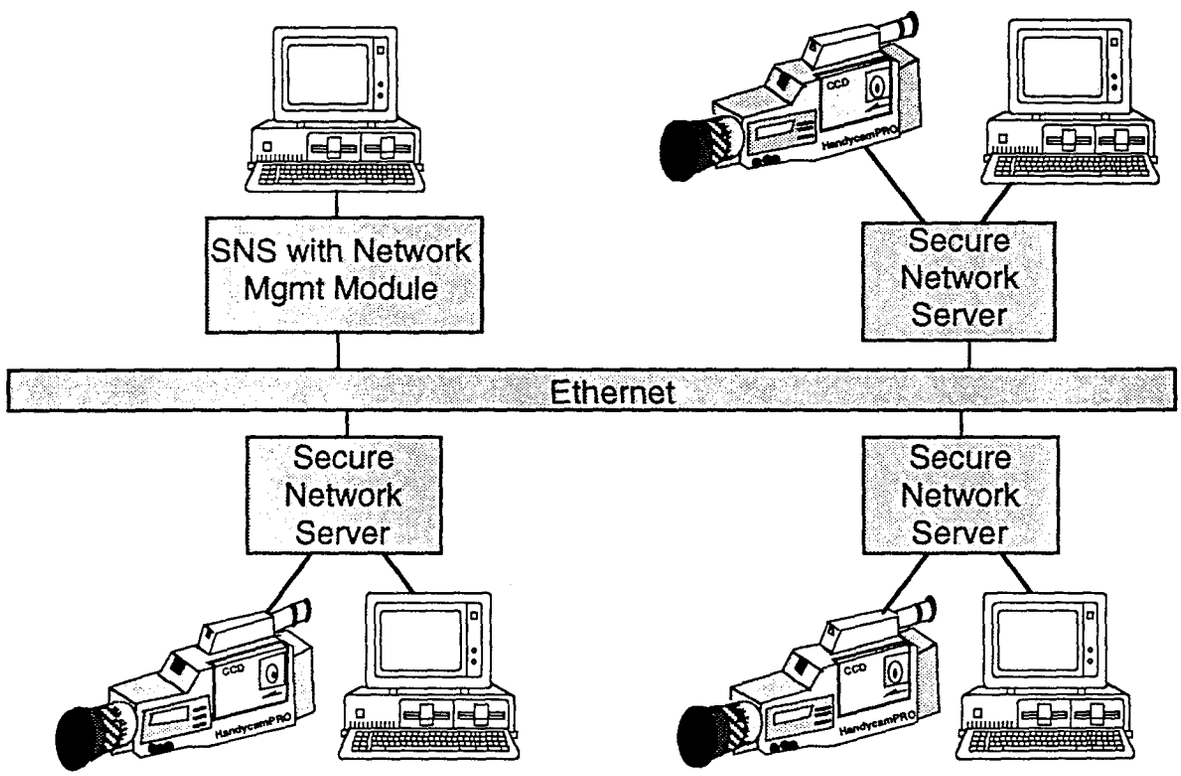


Figure 3-3. Boeing MLS LAN Configuration

Xerox Encryption Unit (XEU) and Xerox Ethernet Tunnel (XET). The XEU is a stand-alone communications device that is inserted between a workstation and a LAN. It performs Type 1 encryption through TS/SCI for Ethernet LANs by implementing proprietary security functionality between the Logical Link Control (LLC) and Media Access Control (MAC) sublayers of the Data Link Layer, much like the IEEE 802.10 Standard for Interoperable LAN/MAN Security (SILS) Secure Data Exchange Protocol (SDE). Similar to SDE (and the EIP discussed earlier), the XEU encrypts the user data field of the frame and bypasses processing of some header and trailer information. The XEU can only be used on an Ethernet LAN. If internetwork routing is required, an Xerox Ethernet Tunnel (XET) can be added to each Ethernet LAN where XEUs are located. The XET prepends IP headers for routing to the destination LAN where the destination XET will strip off the IP header and relay the frame to the destination host.

The XEU is configured by the factory to allow the XEU to process packets from a single secure source (Single Host Mode) or to process packets from multiple secure sources (Multiple Host Mode). The XEU allows up to 1,000 simultaneous network connections. XEU and Non-XEU users share the same Ethernet cable but typically cannot communicate with each other. However, there is a Bypass Key that can be selected to allow information to pass through the XEU without encryption/decryption. This feature enables the XEU user to communicate with non-XEU users, in a non-secure mode, of course.

Users are required to physically insert a Crypto Ignition Key (CIK) into the XEU to activate the device. The NSO must preload the CIK with TEKs. There is no dynamic key management capability. A TEK can be used for pairwise encryption with another station or for entry into a cryptonet where a group of users share the same TEK. Users can communicate in a secure mode only with other stations that are specified by the NSO and at the sensitivity levels specified by the NSO. Multicast and Broadcast addresses are supported.

XEU throughput is approximately 960 Kbps (based on transmission rates of 200 600-byte packets per second). (Xerox claims that the XET has a throughput rate of 3 Mbps, based on 650 600-byte packets per second.)

MISSI Network Security Manager (NSM). The Network Security Manager consists of software applications that will run on COTS workstations supported by CPs or Appliqués. The NSM will manage the security of the MISSI network components within the local subscriber environment (LSE). The NSM will interface with either Internet or ISO protocols. There are five applications that comprise the NSM:

- Local Authority Workstation (LAW) – Provides support for access control permissions, cryptographic key and privilege management, confidentiality, source authentication (through digital signatures), and non-repudiation for the LSE
- Audit Manager (AM) – Collects auditable events for the LSE
- Secure Directory Server (DS) – An X.500-based repository of userids and public key certificates

- Mail List Agent (MLA) – Contains lists of addressees associated with a groupid so that electronic mail can be multicast
- Rekey Manager (RKM) – Works with the EKMS to provide dynamic electronic rekeying for the LSE.

MISSI Secure Network Server (SNS) Fileserver. The SNS, being developed by Secure Computing Corporation, is a multi-CPU COTS workstation that is based on Logical Coprocessing Kernel (LOCK™) technology. It is more highly assured than an Appliqué workstation. The SNS, when used as a fileserver within an LSE, is being designed to allow files of different security levels from Unclassified to Top Secret/SCI to be stored and accessed simultaneously by users on multilevel LANs or multilevel workstations. In addition to being designed to the Trusted Computer System Evaluation Criteria A1 level (though not yet certified), the SNS will provide the option for providing Type 1 encryption of data files. When the CIK is removed, the SNS becomes an unclassified Controlled Cryptographic Item.

3.1.4 WAN Products – Type 1

Type 1 WAN products being reviewed include SNS Guard/Regrader, Radiant Mercury, MISSI In-line Network Encryptor (INE), and SONET and ATM encryptors.

SNS Guard/Regrader. The SNS guard/regrader is an enhanced version of the COTS SNS being developed by Secure Computing Corporation as a fileserver, discussed above. The SNS, when used as a guard/regrader, is being designed to interface multiple protected enclaves operating at different security levels up to Top Secret by providing a *message prerelease review* function. It will provide end-to-end encryption between SNSs to tunnel through unprotected WANs. It will be compatible with the EKMS for dynamic rekeying. The SNS guard/regrader will support electronic mail using SMTP and connectivity to implicitly labeled TCP/IP networks.

Radiant Mercury. Radiant Mercury is intended to be a stand-alone multilevel communications device that is inserted between an SCI network and a GENSER network to provide sanitization, downgrade, and guard functions. It could also be placed between two SCI networks operating under different compartments, or between two GENSER networks operating at different classification levels. Since Radiant Mercury meets only B1 criteria, it cannot actually be used for multilevel connectivity.

The purpose of Radiant Mercury is to support the concept of a worldwide Communications Grid while protecting certain sensitive sources and methods of intelligence collection. Since Radiant Mercury software operates at the Application Layer, it is independent of the communications protocols that operate below it, making it transportable across existing and future communication systems.

MISSI In-line Network Encryptor (INE). One configuration for the In-Line Encryptor, shown in Figure 3-4, is as an end-to-end encryption device which acts as a transport overlay across a WAN. It can be used to provide access control between local area networks. SNS can be added between the LANs and the INEs to serve larger and more varied local networking structures. Multiple layering of security services, such as using INEs with FORTEZZAs and SNSs, would allow Top Secret connectivity. The INE obtains new key material from the Network Security Manger (NSM) Rekey Manager (RKM). INE is a generic term that applies to a number of products including the Motorola Caneware and Motorola Network Encryption System (NES). It can also be used to refer to Synchronous Optical Network (SONET) and Asynchronous Transfer Mode (ATM) encryptors, though these are discussed separately in the following section.

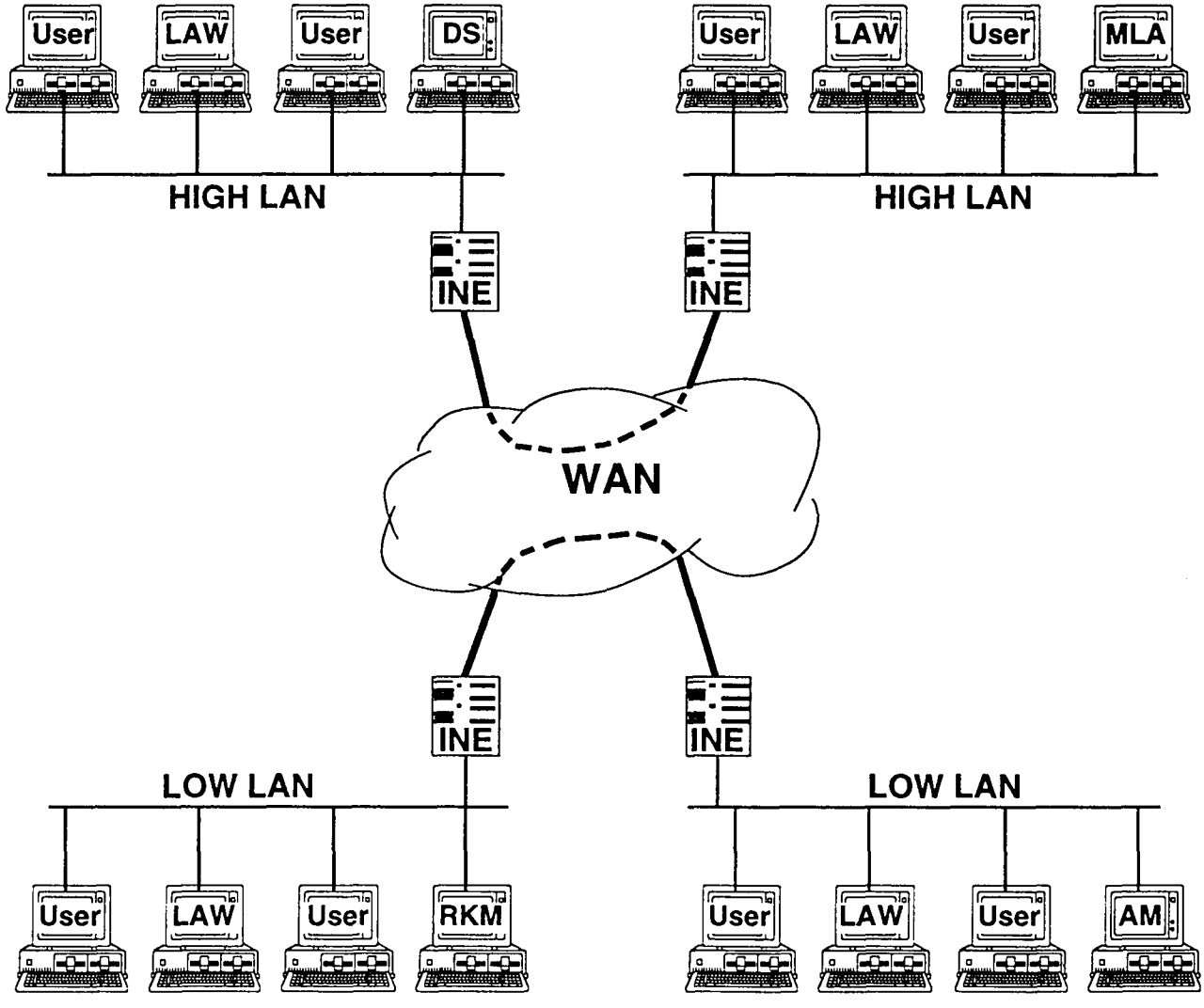


Figure 3-4. In-line Network Encryptor Configuration

Caneware is a stand-alone B2 multilevel communications device that allows the connection of multiple workstations to the network to support up to Top Secret/SCI processing. It supports X.25 and IP with the IP Security Option (IPSO) and allows up to 1,000 network connections. Caneware security services include identification and authentication, mandatory and discretionary access control, Type 1 confidentiality, integrity, and audit. Caneware, like Appliqué and the SNS, is EKMS compatible and uses the SDNS Key Management Protocol (KMP). Caneware encrypts user data and transmits address information needed for routing in the clear. The maximum throughput rate is 750 Kbps.

The NES, shown in Figure 3-5, is a stand-alone communications device that is inserted between a workstation and a LAN, or between two LANs, to protect data on the LANs and WANs. NES services include Type 1 (through Top Secret) encryption/decryption, mandatory and discretionary access control, data integrity, peer-entity authentication, audit, and electronic key management. NES currently supports only single-classification labeling and processing. In the future, Motorola plans to modified the NES to process a range of security levels to support MLS processing.

The red (classified) side of the NES connects to a workstation or an Ethernet LAN, while the black (unclassified) side of the NES connects to Ethernet, Token Ring, FDDI, or X.25 networks. If internetworking is desired, the black side can interface to a DoD (UDP/TCP/IP) network or an ISO (TP4/CLNP) network so that it is an open system for interfacing many hosts and network applications. For security, the NES implements SDNS Security Protocol 3 (SP3) and KMP. Motorola plans to implement SP2 in the NES in the future when IEEE 802.10 Secure Data Exchange protocol is adopted as SP2. The protocol entities are installed on interface cards and can be exchanged as new protocols are developed.

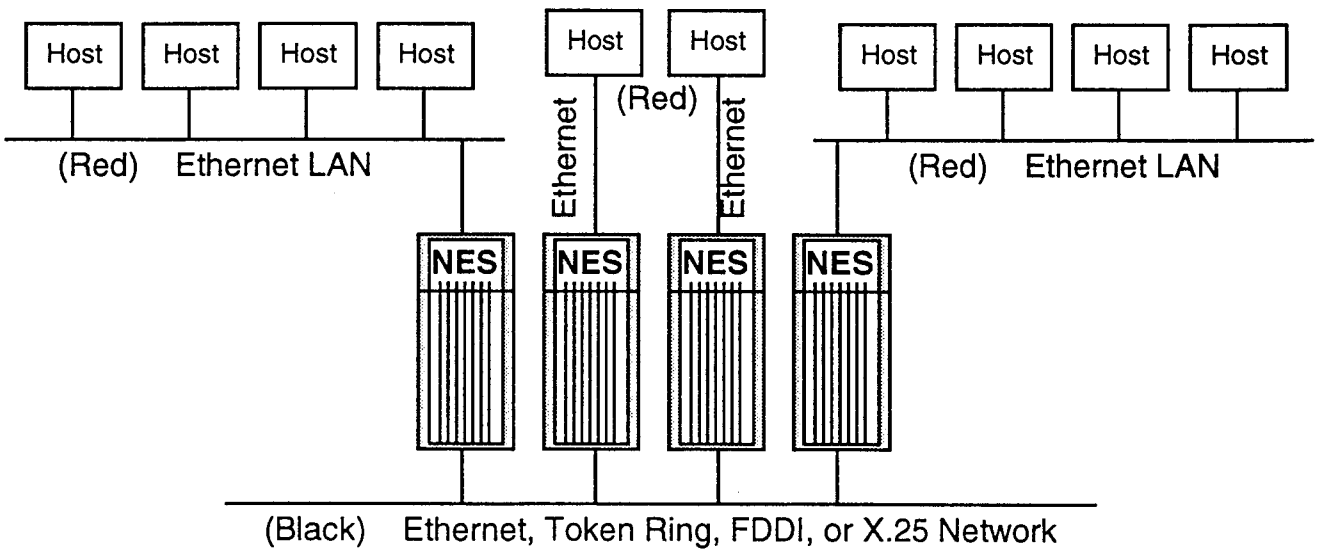


Figure 3-5. Network Encryption System Configurations

When a host on a red network sends a message to a host on another red network, the sending NES encrypts the entire PDU and prepends a new header with the sending NES address as the source address and the receiving NES as the destination address. The NES database maintains identity-based access control lists and an audit trail of failures, problems, and security related incidents.

Operational keying material is provided manually via a key storage device which is identical to that used for STU-III telephones. In addition, NES uses the Firefly Key Exchange Protocol to perform electronic key exchanges with EKMS over the black network and generate TEKs for the communications session between two parties.

NES throughput varies with the network configuration, protocols used, packet sizes, traffic load, and other factors. An approximate rate is 300 to 500 Kbps, with a maximum of 800 Kbps. Motorola is targeting T1 (1.54 Mbps) speeds for the future.

SONET and ATM encryptors. An ATM encryptor, such as the Fastlane (under development), will be useful for multimedia processing because it has no relevant performance limit. Therefore, an ATM encryptor can encrypt information as fast as the media can deliver it. While the ATM encryptor will not decrease throughput, it will add delay for delivery of the traffic. ATM encryptors are key-agile and can thus meet the requirement of being able to encrypt various ATM cells using different keys based on the virtual path indicator (VPI) and virtual channel indicator (VCI).

The KG-189 SONET encryption device will be available before an ATM encryptor and, according to NRL, may be more useful since Naval personnel are familiar and comfortable with link encryption. The KG-189 will have multi-port connectivity, as shown in Figure 3-6 below. Each channel will be designation for single-classification operation, but each channel can be designated at a different level from Secret to Top Secret/SCI. Multiplexing will occur after encryption.

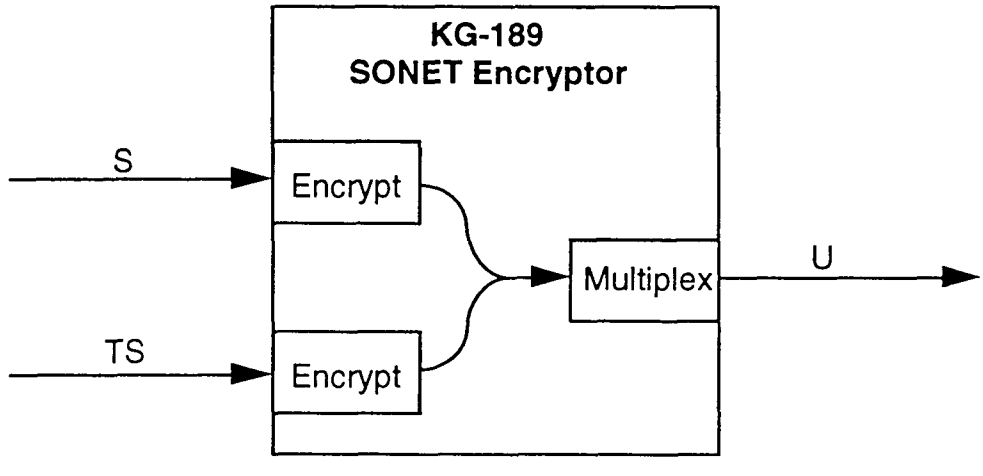


Figure 3-6. KG-189 SONET Encryptor

3.2 Protocol Standards

Two sets of protocols have been standardized. The DoD protocol stack has been considered the *de facto* standard. It is used in the Internet and was developed before the International Standards Organization (ISO) developed their standards. The ISO Open Systems Interconnection (OSI) protocol stack has been considered the *de jure* standard. Foreign governments are rapidly adopting OSI protocols and the U.S. Government has attempted to promote implementation of the OSI protocol stack by mandating (for a while) its use in FIPS PUB 146, Government Open Systems Interconnection Profile (GOSIP). However, implementations of the DoD protocol stack currently greatly exceed those of the OSI stack.

The Federal Interworking Requirements Panel (FIRP) was directed by the President's Office of Management and Budget (OMB) to determine whether OSI or TCP/IP is better for the Government. Members represented DoD, Treasury, Veterans Affairs, Department of Energy, GSA, NASA, NTIA, and the National Science Foundation. The panel found that they could not select between TCP/IP and OSI. Accordingly, they recommended that FIPS 146 be rewritten to include both the IP and OSI suites, as well as proprietary and hybrid stacks. The ultimate goal is to converge to a single interconnected, interoperable standards-based network environment, that is a seamless (i.e., not Government-unique, but what is used in the commercial marketplace) part of the National Information Infrastructure (NII). Proprietary products currently outsell open products. Standards need to address higher layer functionality (e.g., mail directory, file transfers, transaction processing, electronic data interchange, etc.) in order to displace the proprietary protocols and thus systems built around those protocols. Subsequently, the U.S. Government has relaxed the requirements in accordance with the FIRP recommendations.

De facto Standards. The DoD protocol stack includes:

- Simple Network Management Protocol (SNMP)
- Simple Mail Transfer Protocol (SMTP)
- File Transfer Protocol (FTP)
- Telnet Protocol (Remote Logon)
- Transmission Control Protocol (TCP)
- Internet Protocol (IP).

These protocols are widely implemented but may lack capabilities that will be needed in the future, including security capabilities. Internet Protocol, for example, does not have a sufficient address space to meet future needs. Replacement of IP is inevitable. Several options have been implemented, but most are not compatible.

Two additional protocols could be added to the DoD stack, though these have not been implemented outside military environments. DoDIIS Network Security Information

Exchange (DNSIX) and Multilevel Architecture for 'X' Security Information Exchange (MAXSIX) protocols provide CMW operating system extensions at the B1 level. DNSIX/MAXSIX operate at the Network, Transport, and Session Layers to provide datagram security labeling, mandatory access control, auditing, and other security services in a TCP/UDP/IP environment. They do not provide confidentiality. DNSIX is available to government agencies from DIA as GOTS software for DoDIIS networks. MAXSIX is a SecureWare initiative and is being developed by a consortium of vendors.

De jure Standards. The OSI protocol stack includes:

- Common Management Information Protocol (CMIP)
- X.400 Message Handling System (mail)
- File Transfer, Access, and Management Protocol (FTAM)
- Connection Oriented Transport Protocol (TP0, TP1, TP2, TP3, and TP4)
- Transport Layer Security Protocol (TLSP)
- Connectionless Network Protocol (CLNP)
- Network Layer Security Protocol (NLSP).

These protocols are not as widely implemented as the DoD protocols, but may have additional capabilities that will prove useful in the future. Additional protocols are being added to the OSI stack for directory services (X.500), system/security management, key management, and Data Link Layer security (IEEE 802.10 Standard for Interoperable LAN and MAN Security).

3.3 Posture for Protection Against Identified Threats

This study was not intended to analyze the security posture of the existing environment since the analysis of the existing environment could not be performed in sufficient detail. However, based on the limited review of existing products, the following findings are suggested.

DoD networks can no longer remain isolated. Use of commercial products and communications resources must be used. Furthermore, sensitive or classified enclaves must communicate with non-secure unclassified networks in order to gather information needed to accomplish their mission. To compound the problems associated with interconnectivity, the threats from both insiders and outsiders are becoming increasingly sophisticated.

Ten high level security implementation requirements were identified in Section 2. These requirements must be met in future efforts so that suitable networks can be built to permit the interconnectivity necessary to support the user missions.

The capabilities of the products, with respect to the security implementation requirements, are summarized in Table 3-2. These findings provide a general indication of the security posture of the various categories of products and do not indicate the findings for each individual product because the analysis was not at a sufficient depth to determine all the capabilities of each product. The products that have been found to satisfy individual requirements do not come close to simultaneously meeting all of the requirements. The technology is far from being capable of providing all of the security services in a widely used, common manner.

The first high-level requirement calls for the implementation of open system architectures. Connectivity to common carriers dictates standard protocols. This challenge has been accepted almost universally by vendors. The use of proprietary protocols is not being suggested except when they are absolutely necessary. DoD protocols are widely implemented. OSI protocols are being added to some existing products and are being increasingly specified for future products. Security protocol implementations are focusing on recently standardized protocols. Efforts in both the Internet Engineering Task Force (IETF) and ISO standards bodies are attempting to use application programming interfaces (APIs) in order to add security services to the network while preserving existing applications. Security efforts are also attempting to preserve the existing communications stacks to the maximum extent possible.

The second high-level requirement calls for many aspects of interconnectivity. Products needed to provide connectivity in all security modes of operation (dedicated, system high, multilevel, and compartmented) are being developed. Methods are being developed to provide connections between classified and unclassified networks in order to acquire weather, news broadcasts, and other unclassified information needed in the classified environment while at the same time not allowing classified information to transfer to the unclassified side. Since most computers will never be equipped with high assurance security devices, there is be a need for secure systems to interface with non-secure systems. Protocols and devices are being developed that can be bypassed for such communication without introducing high risk covert channels. Distributed client-server architectures allow information to be shared in a manner that enhances service assurance. As such, security must be, and is being, used to support client-server architectures. Multilevel distributed processing necessitates the simultaneous support of multiple security policies at individual workstations and LSEs. Trusted workstations and network security products that support MLS are being developed so that this requirement can be met. Common security management is necessary so that security associations can be established to permit secure communications. Several standardization efforts are currently underway to develop a single security association management protocol that defines the managed objects needed to accomplish security exchanges. Security protocols are being designed with interfaces that can be used with whichever standard is adopted. Finally, reliability and survivability must be built into the standards. This is being done through redundancy, secure relays that isolate portions of the network when needed, distributed servers, and other techniques.

Table 3-2. Comparison of Products and Requirements

	Type 2 W/S and Peripheral Products	Type 1 W/S and Peripheral Products	Type 1 LAN Products	Type 1 WAN Products
• Secure Open Systems Architecture				
– Open system standards				
• Internet (TCP/IP, SMTP, FTP, Telnet, SNMP)	√	√	√	√
• ISO (COTP, CLNP, X.400, X.500, CMIP)	√	√	**F**	**F**
• Security (SDNS MSP, SILS, NLSP, TLSP)	√	**F**	**F**	**F**
– Preserve existing APIs	√	√	√	√
• Interconnectivity and Distributed Processing				
– Interface in all operational security modes	-	√	√	**F**
– Connectivity between classified and unclassified	-	√	- (1)	- (2)
– Connectivity between secure and non-secure	√	-	-	-
– Support distributed client-server architecture	√	√	√	-
– Maintain user and object IDs by security policy	√	√	√	√
– Common security management	√	√	√	√
– Reliability and survivability	√	√	√	√
• Maximize use of COTS/GOTS	√	√	√	√
• Security Processing at Extremely High Speeds	~10 Mbps	TBD	80M (3)	~1 Mbps
• Standards and Interfaces for Multilevel Security	-	√	√	**F**
• Secure User Mobility				
– Allow users to have access from anywhere	√	√	-	-
– Address mobility across subnetworks	-	-	-	-
– Secure wireless technology	-	-	-	-
• Secure Multimedia Communications	-	√	-	- (4)
• Secure Firewalls				
– Front-ends	-	-	√	-
– Relays	-	-	-	√
• Selectable Security Services				
– Identification and Authentication	√	√	√	√
– Access controls	√	√	√	√
– Confidentiality	√	√	√	√
– Integrity	√	√	√	√
– Non-repudiation	√	√	-	-
– Labeling	-	√	√	**F**
– Auditing	-	√	√	√
– Dynamic key management	√	√	√	**F**
• Secure Multicast Routing	√	- (5)	-	**F**

Table 3-2 Notes:

√	Check mark indicates products satisfy the requirement.
-	Dash indicated products do not satisfy the requirement.
(F)	Vendors have indicated plans to meet this requirement in future versions of their product.
(1)	Generally connectivity through the unclassified network is via tunneling. Multilevel connectivity between a classified network sending an unclassified message to an unclassified network is not supported.
(2)	Some WAN interface products support connectivity between classified and unclassified systems, but external technologies are not in place to allow it.
(3)	LAN interface products currently have throughput rates of between 235 Kbps and 2.8 Mbps. However, Verdix claims they will upgrade VSLAN in 1995 to process Ethernet traffic at speeds of 80 to 90 Mbps.
(4)	With the exception of SONET and ATM Encryption devices, the products are not currently designed to provide the speeds necessary for multimedia processing.
(5)	The Message Security Protocol (MSP) specification allows for multiple addressees and is suitable for multicast routing by a routing protocol.

The third high-level requirement calls for maximizing the use of COTS and GOTS hardware and software in order to reduce the cost of developing new products for each mission. Standardization of security frameworks, protocols, and techniques have supported this goal. Vendors are building COTS products based on these standards with the hope of finding a large DoD market.

The fourth high-level requirement calls for security services that function at extremely high speeds. Initially, this means up to 30 Mbps at individual workstations. New LAN protocols that deliver data at speeds nearing 100 Mbps are being developed. The minimum acceptable speed will rise rapidly as multimedia applications are introduced to run at the speeds of ATM. A year ago, it was claimed that ATM may sometime support processing rates of 2.5 Gbps. Today, speeds in excess of 50 Gbps are being discussed. A few security products currently meet the stated requirement of 30 Mbps, and others are being designed to meet 60 to 100 Mbps throughput rates within the next two years. The only high speed products that are focusing on ATM speeds are the KG-189 SONET Encryptor and ATM encryptors such as the Fastlane.

The fifth high-level requirement calls for standards, interfaces, and protocols for multilevel security. Efforts to develop multilevel host operating systems have been underway since before 1983 when the Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, was introduced. Multilevel network efforts are a more recent direction, though there are several products that have been developed to provide that capability. Security protocols have been standardized which support labeling and rule-based access controls. Significant progress is being made in this area.

The sixth high-level requirement calls for user mobility. There are three aspects to this requirement. First, users are no longer accessing their data from a stand-alone host. They are connecting their computer to the network and expecting to be able to access their data from any station in the network. Some security products allow users to possess a Datakey or "smart-card" that can be inserted into any smart-card reader on the network in order to access their data. However, these products have limited application since other organizations are not currently likely to have the same product. This concept is being addressed. Two other aspects of user mobility are more abstract for the time being. First, as users become more mobile, logging onto a session and carrying their computer with them in the car or airplane, or someday on their wrist, they will need the ability to transfer their identity across subnetwork domains without losing the connection and without compromising their security posture. Protocols that can support this level of address mobility are being proposed. However, security may not be addressed in the initial implementations. Finally, security for wireless technology will be needed. Wireless technology generally involves line-of-sight transmission for a hospital, factory, or shipboard environments where cables are a hazard. However, radio frequencies are being proposed. As these standards progress, security must be included.

The seventh high-level requirement calls for secure multimedia communications. This involves the binding of sensitivity labels to the information they represent. In a workstation, this will require labels for multiple windows. The CMW takes an interesting approach by using two types of labels, one to indicate the classification range for the user during the session and one to indicate the sensitivity of a particular window. Communications protocols and products may sometime do the same. Network management must also associate labels with nodes and communications channels. The other aspect of secure multimedia communications relates to separation of payloads on the channel and the speeds that will be needed for multimedia.

The eighth high-level requirement calls for secure firewalls to protect Local Subscriber Environments from penetration and at the same time allow all authorized traffic to pass through. Ideally, security will ultimately be installed in each workstation and server, and there will be no need for a firewall. However, the cost of providing highly secure workstations and servers to the entire user community will prevent this approach from being adopted in the near-term. Therefore, firewalls are necessary in order to allow connectivity of secure subnetworks to non-secure WANs. Some relays have been developed with security filtering properties, but no fully effective firewalls have been developed. There are those who believe that completely effective firewalls can never be built. Others are more optimistic.

The ninth high-level requirement calls for the availability of selectable security services throughout Navy networks. Security protocols have been standardized to provide optional labeling, confidentiality, and integrity. Vendors are currently developing products that support these protocols. Mechanisms have also been developed for authentication, access control, auditing, and dynamic key management. Future products will no doubt be stronger.

The tenth high-level requirement calls for security considerations as multicast routing protocols are developed. Several multicast routing protocols have been implemented and others are currently being designed. Security has not been a significant factor in any of these design efforts. There are several security issues that should be addressed.

This Page Intentionally Left Blank

Section 4

Conclusions and Recommendations

This Page Intentionally Left Blank

4.0 Conclusions and Recommendations

This Task 4 study analyzed the DGSA, MISSI, and Navy Integrated C4I programs in order to determine security implementation requirements for Navy networks. Each program area was evaluated separately, then the resulting requirements were combined into a composite list of high-level requirements.

The analysis then assessed existing and proposed network security products to characterize the current network security environment. The products analysis was performed at a very high level. Therefore, the findings are preliminary and merit further investigation.

Based on this analysis, the following conclusions and recommendations can be made.

4.1 Conclusions

While the product analysis was performed to a limited depth, it appears that there are not adequate security products to meet the requirements for user mobility, multimedia processing, firewalls, and multicast routing.

- Secure User Mobility – As networks become more robust and users become more mobile, users will demand access to their data from any station in the network. The need has unique security requirements that are not addressed for stand-alone systems because many organizations have control of the many security aspects of the network. As computers become more portable, they will at times require broadcast media for connectivity to the network rather than cables. This also introduces unique security requirements. For example, when a computer that is connected to the network in a secure session moves from one domain to another, as would be the case if the computer were moving in an airplane, the network must continue to support the connection yet must modify the connectivity without losing any packets. Likewise, when a computer is carried around a ship, aircraft, hospital, or other workplace, the connection must not be lost or interfered with, and must not interfere with other signals such as radar and navigation. Technology is beginning to address the need for mobility, but security has not been a driving force in the development efforts.

- Secure Multimedia – Multimedia applications are introducing new uses for windows, including the display of graphical and video information. Some trusted workstations are able to apply two types of sensitivity labels to the information they represent, one that indicates the classification range for the user and one that indicates the sensitivity of a particular window. Network security mechanisms also indicate a workstations range of permissible classifications and the classification level for a particular session, but no single mechanisms can accomplish both. Multimedia communications will require such labeling.

There are other security issues that pertain to multimedia. In particular, as multimedia applications are introduced to run at the speeds of ATM, the minimum acceptable transmission speeds will rise rapidly. Security mechanisms must be developed to support these speeds. Some SONET and ATM encryptors are being developed, but higher layer products are needed as well.

- Secure Firewalls – The security community is not in agreement as to whether firewalls are beneficial or detrimental. Some argue that firewalls provide a false sense of security. Since, by definition, some protocols must be permitted to pass traffic through the firewall, that traffic can be dangerous and difficult to protect. For example, electronic mail may be allowed to pass into the protected subnetwork and could deliver a mail bomb. Firewalls have not been designed to prevent such an attack. Remote logon, if permitted, also has the potential for devastating attacks. Others argue that firewalls can filter out specific types of communications that are known to be high risk. Regardless of which camp is correct, firewalls are not currently very effective against sophisticated attacks, but are useful against unsophisticated attacks. Since it is not possible to install adequate security in every user workstation and server, and since interconnectivity is needed for operational purposes, there is an urgent need for secure firewalls, at least for the short-term.

- Secure Multicast Routing – In order to minimize network congestion, multicast techniques are being developed to send one copy of a message across parts of the network and then have routers burst the message into multiple copies for delivery to all intended recipients. This capability is imperative as multimedia applications become more common. As multicast protocols are developed, security issues must be addressed to ensure that routers correctly deliver traffic to all intended users and at the same time do no deliver traffic where it is not intended.

  Other security implications concern the application of security protocols that encrypt the destination address in a protected header. Since the multicast protocol must be able to modify the address entries, it may conflict with the use of an end-to-end security protocol.

4.2 Recommendations

Since the technologies for user mobility and multicast are not stable, it may be premature to attempt to develop security products for these areas. However, participation in the standardization efforts by security engineers is highly recommended. Security products should be developed to meet near-term requirements for the following:

- Secure Multimedia – Multimedia applications are being developed and will soon be in wide use on internetworks. Existing mechanisms that provide security services are not suitable for the wide bandwidth of multimedia, or for providing unique security such as supporting multiple sensitivity labels for video and whiteboard windows.

- Secure Firewalls – Several types of firewalls are urgently needed. Perhaps the most important are Network Layer firewalls (routers). However, there may also be requirements for Data Link Layer firewalls (bridges) or for application specific firewalls that could be installed in-line with current firewalls.

Further studies are needed to assess these areas that appear to be deficient. Additional products are needed to meet the security needs in these two areas. When user mobility and multicast technologies are more stable, security protocols, products, and interfaces will be needed in those areas.

This Page Intentionally Left Blank

Appendices

This Page Intentionally Left Blank

Appendix A

Acronyms

This Page Intentionally Left Blank

Appendix A

Acronyms

ALLPOWER	All Purpose Workstation Security Peripheral
AM	Audit Manager
ANSI	American National Standards Institute
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
C4I	Command and Control, Communications and Computers, and Intelligence
CCC	CINC Command Complex
CIPSO	Commercial Internet Protocol Security Option
CIK	Cryptographic Ignition Key
CLNP	Connectionless Network Protocol
CLTP	Connectionless Transport Protocol
CMIP	Common Management Information Protocol
CMW	Compartmented Mode Workstation
CN	Communications Network
COTP	Connection Oriented Transport Protocol
COTS	Commercial Off-The-Shelf
CP	Crypto-Peripheral
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSS	Communications Support System
DAC	Discretionary Access Control
DCS	Defense Communications System
DES	Data Encryption Standard
DGSA	DoD Goal Security Architecture
DIA	Defense Intelligence Agency
DIS	Defense Information System
DISA	Defense Information Systems Agency
DISSP	DoD Information Systems Security Policy
DNSIX	DoDIIS Network Security Information Exchange
DoD	Department of Defense
DoDIIS	DoD Intelligence Information System
DQDB	Distributed Queue Dual Bus
DS	Directory Server
EHF	Extremely High Frequency
EIP	Embeddable INFOSEC Product
EKMS	Electronic Key Management System
ELF	Extremely Low Frequency
FDDI	Fiber Distributed Data Interface
FTAM	File, Transfer, Access and Management Protocol
FTP	File Transfer Protocol
Gbps	Giga (billion) Bits Per Second

Appendix A – Acronyms (continued)

GENSER	General Service
GLOBIXS	Global Information Exchange System
GOSIP	Government OSI Profile
GOTS	Government Off-The-Shelf
GULS	Generic Upper Layer Security
IBAC	Identity Based Access Control
I&A	Identification and Authentication
IC2	Integrated Interior Communications System
ICV	Integrity Check Value
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	Internet Engineering Task Force
INE	In-line Network Encryptor
INFOSEC	Information Security
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
KDC	Key Distribution Center
KM	Key Management
KMP	Key Management Protocol
LAN	Local Area Network
LAW	Local Authority Workstation
LCS	Local Communications Systems
LDR	Low Data Rate
LEAF	Law Enforcement Access Field
LLC	Logical Link Control
LOCK™	Logical Coprocessing Kernel
LSE	Local Subscriber Environment
MAC	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MAXSIX	Multilevel Architecture for 'X' Security Information Exchange
Mbps	Mega (million) Bits Per Second
MHS	Message Handling System
MIC	Message Integrity Check
MISSI	Multilevel Information Systems Security Initiative
MLA	Mail List Agent
MLS	Multilevel Security
MSP	Message Security Protocol
NCCOSC	Naval Command, Control, and Ocean Surveillance Center
NES	Network Encryption System
NKDS	Navy Key Distribution System
NLSP	Network Layer Security Protocol
NMM	Network Management Module

Appendix A – Acronyms (continued)

NRaD	NCCOSC RDTE Division
NRL	Naval Research Laboratory
NSA	National Security Agency
NSC	Network Security Center
NSD	Network Security Device
NSO	Network Security Officer
NSM	Network Security Manager
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
OSI RM	OSI Reference Model
OTAR	Over-the-Air Rekeying
PCMCIA	Personal Computer Memory Card International Association
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIN	Personal Identification Number
RBAC	Rule Based Access Control
RDTE	Research, Development, Test, and Evaluation
RI-PEM	Riorden Privacy Enhanced Mail
RKM	Rekey Manager
SAID	Security Association Identifier
SBIR	Small Business Innovative Research
SCI	Sensitive Compartmented Information
SCSI	Small Computer System Interface
SDE	Secure Data Exchange Protocol
SDNS	Secure Data Network System
SDS	Secure Directory Server
SDU	Service Data Unit
SESE	Security Exchange Service Element
SEW	Space and Electronic Warfare
SILS	Standard for Interoperable LAN and MAN Security
SLP	Single Link Procedures
SMIB	Security Management Information Base
SMP	Security Management Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNS	Secure Network Server
SONET	Synchronous Optical Network
SP2	Security Protocol 2
SP3	Security Protocol 3
SP4	Security Protocol 4
SP7	Security Protocol 7
SPAWAR	Space and Naval Warfare Systems Command
TADIXS	Tactical Data Information Exchange System
TCC	Tactical Command Center
TCP	Transmission Control Protocol

Appendix A – Acronyms (continued)

TEED	Tactical End-to-End Encryption
TEK	Traffic Encryption Key
TIS-PEM	Trusted Information Systems Privacy Enhanced Mail
TIU	Trusted Interface Unit
TLSP	Transport Layer Security Protocol
TP0	Connection Oriented Transport Protocol, Class 0
TP1	Connection Oriented Transport Protocol, Class 1
TP2	Connection Oriented Transport Protocol, Class 2
TP3	Connection Oriented Transport Protocol, Class 3
TP4	Connection Oriented Transport Protocol, Class 4
UDP	User Datagram Protocol
VCI	Virtual Channel Indicator
VPI	Virtual Path Indicator
VSIP	Verdix Secure Internet Protocol Router
VSLAN	Verdix Secure LAN
WAN	Wide Area Network
XET	Xerox Ethernet Tunnel
XEU	Xerox Encryption Unit

Appendix B

DoD Goal Security Architecture (DGSA) Security Policy and Derived Security Requirements

This Page Intentionally Left Blank

Appendix B

DGSA Security Policy and Derived Security Requirements

a. Multiple Information Security Policy Support. DoD information systems must support information processing under multiple security policies of any complexity or type, including those for sensitive unclassified information and multiple categories of classified information. [DGSA 93, section 2.1(1)]

-- Allows users to operate simultaneously at multiple sensitivity levels or under multiple security policies (e.g., by using multilevel secure systems) on a single device (e.g., workstation, outboard protocol device). [DGSA 93, section 2.2.1]

-- Implementations must provide users with confidence that there will not be any security policy violations. [DGSA 93, section 2.2.1]

Derived Requirements:

1. The ability to support (enforce) each security policy independently of other security policies supported in shared information systems and communications systems is required. [DGSA 93, section 2.3.1.1]

2. The information systems must reliably maintain the identities of users and information objects under each security policy. [DGSA 93, section 2.3.1.1]

3. All references by users (or processes representing them) to information objects must be mediated by a reference monitor in order to provide data confidentiality and integrity. (Note that any number of reference monitor implementations may be possible.) [DGSA 93, section 2.3.1.1]

4. When information processing operations are supported by distributed information processing systems, the security policy enforcement for information in transit is commonly supported by mutual authentication, access control, data integrity, data confidentiality, and non-repudiation communications security services. [DGSA 93, section 2.3.1.1]

5. The integration of voice, imagery (fax), and data requires a secure display (windows) implementation. [DGSA 93, section 2.3.2.1]

6. It is highly desirable that security features become standard elements of commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) equipment. [DGSA 93, section 2.3.2.2]

7. A secure information system must isolate its sensitive information and protect it with its own security mechanisms. [DGSA 93, section 4.2.2]

Appendix B – DGSA Security Requirements (continued)

b. Open Systems Employment. DoD information systems must be sufficiently protected to allow distributed information processing (including distributed information system management) among multiple hosts on multiple networks in accordance with open system architectures. [DGSA 93, section 2.1(2)]

-- Users operating under different security policies may need to share components. [DGSA 93, section 2.2.2]

-- Complex policies for sharing and transferring information among users operating under different security policies must be supported. [DGSA, sec. 2.2.2]

-- DoD information systems must be open in the sense that potential connectivity among them is always supported, even if a particular request for communication is denied because of a security policy decision. [DGSA 93, section 2.2.2]

Derived Requirements:

8. The user must be able to convey information to another user (or process) that will become the basis for decisions about what (if any) kinds of interaction will be allowed. [DGSA 93, section 2.3.1.2]

9. Standards for the representation and exchange of information, some as part of the communications exchanges and some through security management-related exchanges, are needed. International, national, or DoD (not proprietary) standard protocols, information, and mechanisms will enable users to determine the capabilities and environment of other users or system processes with which they attempt to communicate. (Exception: some tactical systems will use unique standards.) [DGSA 93, section 2.3.1.2]

10. Connectivity to common carriers dictates standard protocols. This standardization includes authentication information, security protocols, key management and distribution, and security management information. [DGSA 93, section 2.3.2.3]

11. ISO 7498-2 [ISO 89A] is adopted by the DGSA, along with the additions and modifications for local area network security (developed in the IEEE 802.10 committees) and the security protocols that are adopted by the ISO community. [DGSA 93, section 4.2.2.3]

Appendix B – DGSA Security Requirements (continued)

12. The SDNS Message Security Protocol (MSP) is the DoD standard for electronic messaging. [DGSA 93, section 7.2.3] MSP will be the basis for secure messaging in Phase II of the Defense Message System. MSP can provide authentication, access control, message confidentiality and integrity, and non-repudiation security services. MSP allows delivery of the same message to multiple recipients supported by several end systems without creating multiple copies of the message in the originating end system. [DGSA 93, section 7.1.2]

13. Provide authentication service. [DGSA 93, section 2.3.1.5] Information systems must have adequate local authentication schemes and security management mechanisms that free the user from the burdens of procedures such as multiple logins. Users wish to be able to be authenticated once to the local system and then transparently interact with the other systems to access resources. [DGSA 93, section 2.3.2.3]

14. Provide access control service. [DGSA 93, section 2.3.1.5]

15. Provide availability service. [DGSA 93, section 2.3.1.5] (Note: Security availability services must be provided in addition to system and network availability services.)

16. Information systems with highly sensitive information must be able to communicate with non-secure as well as secure information systems. [DGSA 93, section 4.2.2]

17. Local Subscriber Environments (LSEs) are defined to include all devices and communication systems under user organization control. Requirements for complete Traffic Flow Security between LSEs must be examined very carefully when one end of the network link terminates in the commercial control zone and address information is needed by the switches in the commercial control zone. One consequence is that the link cannot be used for any other purpose and, thus, creates a closed, protected system. This may be contrary to requirements for open systems. [DGSA 93, section 4.1.2.1]

18. Communications Networks (commercial and DoD) must provide an agreed level of responsiveness, continuity of service, and resistance to threats to availability and integrity. Communications Networks are not relied upon for information confidentiality or integrity (although the network must provide some integrity). Failures in Communications Networks can only result in delay, misdelivery, or non-delivery. [DGSA 93, section 4.2.1]

Appendix B – DGSA Security Requirements (continued)

c. Appropriate Security Protection. DoD information systems must support information processing among users with different security attributes employing resources with varying degrees of security protection, including users of non-secure resources if a particular mission so dictates. [DGSA 93, section 2.1(3)]

-- The appropriate security protection methods can only be determined by those persons responsible for the particular information and who are able to assess its value and the threats to it. [DGSA 93, section 2.2.3]

-- Specific means must be available to users to invoke security mechanisms appropriate to the task at hand. [DGSA 93, section 2.2.3]

-- When common carrier communications must be used, the information systems must be prepared to provide all of the appropriate security protection. The only service that should be assumed from a common carrier communications system is availability. [DGSA 93, section 2.2.3] Availability is the only security service allocated to Communications Networks and Local Communications Systems. [DGSA 93, section 7.0]

Derived Requirements:

19. Security mechanisms must be identified that implement security services at the level of protection required in security policies. [DGSA 93, section 2.3.1.3]

20. Since some security mechanisms may be used to provide (parts of) multiple security services and some security services may be implemented by multiple mechanisms, a determination must be made that the mechanisms are appropriate individually and in combination. The determination must be made by the owners of mission information, or the accreditor who represents the owners. [DGSA 93, section 2.3.1.3]

d. Common Security Management. DoD information systems must be sufficiently protected to allow connectivity via common carrier (public) communications systems. [DGSA 93, section 2.1(4)]

-- The DGSA must address common security management. This commonality will allow security administrators to manage, in a uniform manner, systems that operate under multiple security policies. [DGSA 93, section 2.2.4]

Appendix B – DGSA Security Requirements (continued)

Derived Requirements:

21. The basic elements that must be managed are users, access rights, security policies, information, information processing systems, and the security functions that support the security mechanisms (automated, physical, personnel, or procedural) used to implement security services. [DGSA 93, section 2.3.1.4]

22. The managed objects that constitute each of these elements must be identified and maintained. Users must be known and registered, their access rights determined, the security policies must be represented and maintained, and information objects must be identified and maintained. [DGSA 93, section 2.3.1.4]

23. The format for presenting the information in managed objects and operations on them must be standardized. [DGSA 93, section 2.3.1.4]

24. There must be no security-relevant distinction made among the information objects in an information domain. Each information domain is identified uniquely. The unique identification indicates (directly or indirectly) the sensitivity of all the information objects in the information domain. [DGSA 93, section 4.3.1]

25. Management protocols to accommodate all management exchanges are needed. Common Management Information Protocol (CMIP) or the Simple Network Management Protocol (SNMP) version 2 are currently the best available choices, but the Generic Upper Layer Security (GULS) Security Exchange Service Element Protocol (SESE) could become a critical tool in the future. As the GOSIP position on management protocols becomes stable, the DGSA will adopt the protocols. [DGSA, section 6.2.5]

26. Security mechanism management functions include:

    a. Key management
    b. Encipherment management
    c. Digital signature management
    d. Access control management
    e. Data integrity management
    f. Authentication management
    g. Traffic padding management
    h. Routing control management
    i. Notarization management
    j. Availability management. [DGSA 93, section 6.2.8]

This Page Intentionally Left Blank

Appendix C

Multilevel Information Systems Security Initiative (MISSI) Security Requirements

This Page Intentionally Left Blank

Appendix C

MISSI Security Requirements

1. Capable of having open systems interface with allied and non-allied systems and support networks in the system high, dedicated, multi-level, and compartmented operational modes. Capable of communicating with non-MISSI (untrusted system high) components and allowing connection of networks of differing classification levels (e.g., SECRET Systems High to TOP SECRET MLS). [MISSI 93A, section 1.2]

2. Operate within existing network protocol standards. [MISSI 93A, section 1.2]

3. Decentralize and replicate critical processes to reduce the effect of targeting by hostile or inadvertent attacks. Detect and recover from such attacks. Interacting processes must be mutually suspicious of one another. [MISSI 93B, section 4.3.3.1.2]

4. Assign system privileges commensurate with users needs as established at their instance of registration and authentication. This set of privileges shall be the most restrictive that allows efficient performance of authorized tasks. [MISSI 93A, section 2.2.2, and MISSI 93B, section 4.3.4]

5. Uniquely identify and authenticate individual subjects prior to allowing access to specific objects. Reflect the subject's access rights to individual objects. [MISSI 93B, section 4.3.4]

6. Preserve separation of objects based on their classification; implement trusted operating system software in the workstation, provide a network guard, and provide security services for exchanging information. [MISSI 93A, section 2.2.2]

7. Failure of components must not significantly impact the overall system or network performance, availability, or reliability. System failures and restoration must result in the system continuing in a secure state. Contingency plans must address actions to mitigate threats, recovery from failure situations, and backup operations during recovery. [MISSI 93A, section 1.3.3, and MISSI 93B, section 4.3.3]

8. Detect and notify appropriate users of the existence of dangerous or undesirable security conditions. [MISSI 93B, section 4.3.3.3.2]

9. Ensure and periodically validate the correct operation of system security features and mechanisms. [MISSI 93B, section 4.3.5.1]

Appendix C – MISSI Security Requirements (continued)

10. Continue to function properly while under attack by unauthorized users. [MISSI 93B, section 4.3.11]

11. Security enhancements must run in conjunction with COTS products, must maximize use of existing user equipment and applications, and shall not impede the current user functions. [MISSI 93A, section 1.2]

12. Incorporate firewalls to minimize the effect of intentional subversion or blocking of system communication channels, and limit the damage caused by users (unauthorized and authorized) attempting to overrun, sabotage, or compromise security critical elements or functions. [MISSI 93B, sections 4.3.1.3 and 4.3.2]

13. Protect resources from the threats of theft, espionage, unauthorized disclosure, tampering, unauthorized modification, alteration, manipulation, and denial of service. [MISSI 93B, section 4.3.1]

14. Ensure that information and assets are accessed only by authorized subjects and used for the accomplishment of authorized tasks. Access privileges will be limited to subjects with formal access approval based on parameters specified by the ISSO. Access will be denied following a number of unsuccessful authentication attempts. [MISSI 93B, sections 4.3.1.2 and 4.3.2.1.1]

15. Ensure the confidentiality of the system's information and assets. [MISSI 93A, section 1.3.4, and MISSI 93B, section 4.3.1]

16. Associate actions performed by a subject with that subject. [MISSI 93B, section 4.3.4.2.5]

17. Ensure the integrity of assets and objects: [MISSI 93A, section 1.3.5, and MISSI 93B, sections 4.3.2 and 4.3.3]

    - Act upon processing and routing restrictions to prevent loss of data integrity
    - Detect data alterations that occur during data transfers
    - Detect data alterations that occur when data passes between MISSI components
    - Notify users when data alteration has been detected.

18. Provide proof of information transfer (non-repudiation) as both proof-of-delivery and proof-of-origin. [MISSI 93A, sections 1.3.1 and 2.2.2, and MISSI 93B, section 4.3.4]

Appendix C – MISSI Security Requirements (continued)

19. Ensure only authorized changes to data, information, or processes occur, that they are made by certified processes, and that they are verified, documented, and maintained throughout the operational life of the system. [MISSI 93B, section 4.3.2]

20. Maintain an audit trail of all security relevant events and actions. Ensure that the security audit database can only be accessed by the system auditor. Support the suspension of operations due to the detection of specified security relevant events. [MISSI 93B, sections 4.3.3.3.1 and 4.3.4]

21. Implement electronic key management system (EKMS) compliant services including: seed key conversion, rekey, and distribution of certificate revocation lists. [MISSI 93A, sections 1.2 and 2.2.2]

22. Incorporate security mechanisms to ensure: [MISSI 93B, sections 4.3.1, 4.3.2, 4.3.3, and 4.3.4]

    - Cooperating subjects are operating in a common object security domain
    - Failure of one security mechanism shall not result in the failure of another
    - Establishment of asset values based on time of creation, storage time, required time of delivery, or duration
    - Authorized entities are allowed to establish or change sensitivity attributes of assets
    - Detection and protection of malicious and inadvertent alteration
    - Detection and notification of the existence of unauthorized access or intrusions
    - Monitoring and diagnosis of the nature of system problems or failures
    - Monitoring of identified security channels or processes
    - Detection of unauthorized operations or system failure
    - Performance of liveness checks
    - Performance of security functions within a predetermined period of time
    - Restriction on the use of system resources
    - Traceability of all security relevant events to individual users, processes, or interfaces
    - Protection against mandatory security policy violations.

This Page Intentionally Left Blank

Appendix D

Navy Integrated C4I Security Requirements

This Page Intentionally Left Blank

Appendix D

Navy Integrated C4I Security Requirements

1. Open system standards for securing communications and sharing computing resources are required. [GRUM 92, section 2.1]
   - Provide or improve interoperability with joint-service systems. [SPAWAR 94]
   - To avoid changing existing applications, the existing application programming interfaces (APIs) should be preserved, and Integrated C4I user level security must not be placed at the Application layer or the Presentation layer. [NRL 93A, section 3.0]
   - The Integrated C4I TADIXS will offer the ability to dynamically share communications channels among user communities. The approach is based on mechanisms that are compatible with open systems technology and are placed where there is minimal impact on existing and anticipated applications. [NRL 93A, section 1.0]
   - The (IC)2 program office has established TCP/IP as the baseline (IC)2 communications architecture. The network services provided under TCP/IP include FTP (file transfer), SMTP (electronic mail), and Telnet Protocol (remote login). The communications architecture will evolve to GOSIP as finalized standards, commercial technology, and a strong support base emerge. [NAVSEA 93, section 3.3.2.1]
   - Widespread use of GOSIP will provide important benefits. [SPAWAR 91A, section 4]
   - The Integrated Interior Communications and Control (IC)2 program plan introduces a program to achieve an (IC)2 architecture based on Broadband Integrated Services Digital Network (BISDN) networks executing GOSIP protocols with interfaces to applications running in the POSIX environment on the 2010 combatant. [NAVSEA 93, section 1.3]
   - Permit the use of multi-vendor commercial components in Navy systems by establishing standard component interfaces. SAFENET's OSI Suite is based on the GOSIP protocol set. [GRUM 92, section 2.2.1]
2. Connections between processing environments that operate at different security levels are provided by one-way links from the lower level environment to the higher level environment. One-way communications services may be desired which would be assured by trusted protocols. [GRUM 92, section 2.1]

Appendix D – Navy Integrated C4I Security Requirements (continued)

3. Provide a worldwide Surveillance Grid of sensors and a worldwide Communications Grid of display tools and communications pathways which is focused on the Space and Electronic Warfare commander. [CNO 93]

4. Secure automated connectivity, primarily for electronic mail and file transfer, between classified and unclassified systems and networks is required. [SPAWAR 94]

5. The $(IC)^2$ must be capable of networking mainframes, workstations, and personal computers. [NAVSEA 93, section 3.3.2.1] Support client-server architecture and distributed processing [SPAWAR 94]

6. Integrated C4I TADIXS shall identify all classified or sensitive information before disclosure of that information outside the Integrated C4I TADIXS INFOSEC boundary (e.g., provide assurance). [SPAWAR 92A, section 3.5]

7. There must be timely delivery of data. [Data Access Security Requirements, NRL 93B]

8. Reliable, survivable, and secure communication architecture within a ship is required. [NAVSEA 93, section 3.3]

9. Integrated C4I TADIXS shall protect against denial of service (e.g., assure availability). [SPAWAR 92A, section 3.3]

10. The Navy will continue to require a modest amount of the anti-jam capability inherent in EHF low data rate SATCOM. The Navy must improve the means to switch traffic from one RF asset to another – a key requirement in a jamming environment. [SPAWAR 91A, section 6]

11. Maximize use of COTS. [SPAWAR 94]

12. Encryption currently imposes performance constraints that prevent its use as the confidentiality mechanism in high performance systems. Alternate mechanisms need to coexist with encryption in places where they can be used. [GRUM 92, section 6.2] These mechanisms include protected distribution systems and protected fiber techniques. Performance requirements associated with real-time operations will have a major impact on the design of the network security architecture. Peak data rates in excess of 30 Mbps may need to be supported at particular workstations. [GRUM 92, sec. 2.1]

Appendix D – Navy Integrated C4I Security Requirements (continued)

13. The primary goal of the Integrated C4I architecture is to facilitate multi-level secure information exchange. [NRL 93A, section 1.0] Multilevel secure communications and processing are required. [GRUM 92 section 2.1] Unclassified through TS/SCI [SPAWAR 94]

14. Users should be able to access any information (from within any community necessary) required to do their job. [NRL 93B]

15. Security support for mobile and wireless network technologies will become necessary for efficient operations as these technologies evolve. [TBS]

16. Implement secure displays (windows) for integrated multimedia (voice, imagery, data, video). [TBS]

17. Partition LANs into communities of interest in order to reduce congestion, improve response times, facilitate addition, deletion, and movement of components, facilitate diagnosis and isolation of network problems, and improve confidentiality. [TBS]

18. The security services provided for Naval applications must be sufficient to counter the wide variety of threats including:

    - Eavesdropping (disclosure)
    - Message Modification (intentional)
    - Message Replay
    - Traffic Flow Analysis
    - Impersonation (masquerade)
    - Denial of Service (intentional). [GRUM 92, section 3.1]

    In order to counter the various threats outlined above, corresponding security services must be provided by the network architecture:

    - Authentication
    - Access Control
    - Data Confidentiality
    - Data Integrity
    - Non-Repudiation. [GRUM 92, section 3.2]

Appendix D – Navy Integrated C4I Security Requirements (continued)

19. There must be assurance that the data is genuine, i.e., the indicated source is the true source (authentication). [Data Access Security Requirements, NRL 93B]

20. Integrated C4I TADIXS shall control access to information, services, and equipment. [SPAWAR 92A, section 3.1]

21. Hardware and software based access controls are needed to enable a security administrator to selectively prohibit communication paths which violate the system security policy. [GRUM 92, section 2.1]

22. Integrated C4I TADIXS shall ensure the confidentiality of classified and sensitive user information, system control information, and system security information. [SPAWAR 92, section 3.1] Access to data must be limited to those authorized (confidentiality). [Data Access Security Requirements, NRL 93B]

23. Integrated C4I TADIXS shall maintain the integrity of information, software, and equipment. [SPAWAR 92, section 3.2] There must be assurance that the data is intact (integrity). [Data Access Security Requirements, NRL 93B]

24. There must be sender and receiver non-repudiation. [Data Access Security Requirements, NRL 93B]

25. Any network service that is subject to mandatory access control must have at least the following label properties:

    - A security label must be directly or indirectly associated with each service data unit that is exchanged as a part of the service
    - One or more security labels must be directly or indirectly associated with the network entities that are clients of the service. [GRUM 92, section 6.3]

26. There must be confidence that any associated security labels are correct (i.e., label/data binding and integrity). [Data Access Security Requirements, NRL 93B]

27. True user-to-user (writer-to-reader) security is needed. [NRL 93B] Protection of user data while in transit between users needs to be provided on a user-to-user basis rather than on a node-to-node basis. [NRL 93A, section 2.0] The Transport Layer is the lowest protocol layer that is uniquely user-to-user. User level information security mechanisms implemented at the Transport Layer offer true user-to-user data confidentiality, authentication, and integrity without having to add security to each application. [NRL 93A, section 3.0]

Appendix D – Navy Integrated C4I Security Requirements (continued)

28. Integrated C4I TADIXS shall maintain an audit trail to support the traceability of all security-relevant events (e.g., provide accountability). [SPAWAR 92A, section 3.4]

29. There must be assurance that interconnected systems do not reveal too much information about users and their mission (i.e., traffic flow security). [Data Access Security Requirements, NRL 93B] Traffic flow confidentiality and maintenance of integrity and availability of the communications infrastructure is solvable using traditional COMSEC mechanisms (e.g., link and subnetwork encryption). [NRL 93A, section 2.0] Traffic flow security is not currently achievable with respect to SAFENET, as well as local area networks. [GRUM 92, section 6.1.4]

30. There must be dynamic key management. [Data Access Security Requirements, NRL 93B]

31. Security services for multicast communications will be essential. [GRUM 92, section 2.1]

This Page Intentionally Left Blank

Appendix E

References

This Page Intentionally Left Blank

Appendix E

References

[ADAMS 94] C. Adams, *Security Initiative for Defense Nets Takes Small Steps Forward,* Federal Computer Week, July 25, 1994, pp. 20-22.

[ANSI 88A] American National Standards Institute, *Digital Hierarchy – Optical Interface Rates and Formats Specification,* ANSI T1.105-1988, (Synchronous Optical Network – SONET), ANSI T1X1.5, 1988.

[ANSI 88B] American National Standards Institute, *Digital Hierarchy – Optical Parameters,* ANSI T1.106-1988, (SONET), ANSI T1X1.5, 1988.

[ANSI 89] American National Standards Institute, *Addendum to ANSI T1-105-1988, Digital Hierarchy – Optical Interface Rates and Formats Specification,* (Phase 2 SONET), ANSI T1X1.5, 1989.

[CHES 94] W.R. Cheswick and S.M. Bellovin, *Firewalls and Internet Security - Repelling the Wily Hacker,* Addison-Wesley, Reading, MA, 1994.

[CLIPPER 93] Mykotronx, Inc., *Clipper Family: A New Breakthrough in Encryption Technology,* October 1993.

[CNO 93] Chief of Naval Operations, *Sonata Overview,* circa June 1993.

[DCA 91] Defense Communications Agency, MLS Technology Insertion Program, *Technical Memorandum – Target Architecture and Implementation Strategy for the Joint MLS Technology Insertion Program,* March 1991.

[DGSA 93] Center for Information System Security, Defense Information System Security Program (DISSP), *Department of Defense (DoD) Goal Security Architecture (GOAL), Version 1.0,* Draft, August 1, 1993.

[DIGIRO 91] V. DiGirolamo, *Naval Command and Control: Policy, Programs, People & Issues,* AFCEA International Press, 1991 (forward by Vice Admiral Jerry O. Tuttle).

[DISA 93] Defense Information Systems Agency, Joint Interoperability and Engineering Organization, *Standard Mail Guard (SMG) Functional Requirements Document,* Coordination Draft, October 29, 1993.

Appendix E – References (continued)

[FORD 94] W. Ford, *Computer Communications Security – Principles, Standard Protocols and Techniques,* Prentice Hall, Englewood Cliffs, NJ, 1994.

[GRUM 92] Grumman Data Systems, *Secure SAFENET Communications,* NRaD Contract N66001-90-D-0192, June 30, 1992.

[HALSALL 92] F. Halsall, *Data Communications, Computer Networks and Open Systems*, Third Edition, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[IEEE 90] Institute of Electrical and Electronics Engineers, *IEEE Standard for Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network*, IEEE Standard 802.6, 1990.

[IEEE 93] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS), Currently Contains Secure Data Exchange (SDE) (Clause 2)*, IEEE Standard 802.10-1992, February 5, 1993.

[IEEE 94] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) Clause 3 — Key Management Protocol,* Unapproved Draft IEEE 802.10c/D5, June 8, 1994.

[ISO 84] International Standards Organization, *Information Processing Systems — Open Systems Interconnection Basic Reference Model,* ISO 7498, October 1984.

[ISO 88A] International Standards Organization, *Information Processing Systems—Open Systems Interconnection — File Transfer, Access, and Management – Part 1: General Introduction*, ISO 8571, October 1988.

[ISO 88B] International Standards Organization, *Information Processing Systems—Open Systems Interconnection — Connection Oriented Transport Protocol Specification*, ISO 8073, December 15, 1988.

[ISO 89A] International Standards Organization, *Information Processing Systems — Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture,* ISO 7498-2, February 1989; also ITU-T Recommendation X.800.

[ISO 89B] International Standards Organization, *Information Processing Systems—Fiber Distributed Data Interface (FDDI)— Part 1: Physical Layer Protocol (PHY)*, ISO 9314-1, April 1989.

Appendix E – References (continued)

[ISO 89C] International Standards Organization, *Information Processing Systems—Fiber Distributed Data Interface (FDDI)— Part 2: Token Ring Media Access Control*, ISO 9314-2, June 1989.

[ISO 90A] International Standards Organization, *Information Processing Systems—Fiber Distributed Data Interface (FDDI)— Part 3: Physical Layer Medium Dependent (PMD)*, ISO 9314-3, October 1990.

[ISO 90B] International Standards Organization, *Information Processing Systems—Local Area Networks— Part 4: Token-Passing Bus Access Method and Physical Layer Specification*, ISO/IEC 8802-4, 1990; ANSI/IEEE Std 802.4.

[ISO 90C] International Standards Organization, *Information Processing Systems—Data Communications – X.25 Packet Level Protocol for Data Terminal Equipment*, ISO 8208, 1990; also CCITT Recommendation X.25.

[ISO 90D] International Standards Organization, *Information Processing Systems—Common Management Information Protocol Specification*, ISO 9596, 1990.

[ISO 92A] International Standards Organization, *Information Technology — Local and Metropolitan Area Networks – Part 5: Token Ring Access Method and Physical Layer Specification,* ISO/IEC 8802-5, 1992; ANSI/IEEE Std 802.5.

[ISO 92B] International Standards Organization, *Information Technology — Protocol for Providing the Connectionless-Mode Network Service,* ISO/IEC 8473-1, 1992; also ITU-T Recommendation X.233.

[ISO 93A] International Standards Organization, *Information Processing Systems – Local and Metropolitan Area Networks – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification,* ISO/IEC 8802-3, 1993; ANSI/IEEE Std 802.3.

[ISO 93B] International Standards Organization, *Information Technology – Information Retrieval, Transfer and Management for OSI, Generic Upper Layer Security (GULS) – Part 1: Overview, Models and Notation,* ISO/IEC 11586-1, 1993.

Appendix E – References (continued)

[ISO 93C] International Standards Organization, *Information Technology – Information Retrieval, Transfer and Management for OSI, Generic Upper Layer Security (GULS) – Part 2: Security Exchange Service Element (SESE) Service Definition,* ISO/IEC 11586-2, 1993.

[ISO 93D] International Standards Organization, *Information Technology – Information Retrieval, Transfer and Management for OSI, Generic Upper Layer Security (GULS) – Part 3: Security Exchange Service Element Protocol Specification,* ISO/IEC 11586-3, 1993.

[ISO 93E] International Standards Organization, *Information Technology – Information Retrieval, Transfer and Management for OSI, Generic Upper Layer Security (GULS) – Part 4: Protecting Transfer Syntax Specification,* ISO/IEC 11586-4, 1993.

[ISO 94A] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Network Layer Security Protocol,* ISO/IEC 11577, Final text accepted November 1993. International standard published 1994.

[ISO 94B] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol,* ISO/IEC 10736, Final text accepted November 1993. International standard published 1994.

[ISO 94C] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol (Amendment 1 - Security Association Protocol),* Final text accepted November 1993. International standard published 1994.

[ITU 91] International Telecommunications Union – Telecommunications Sector (formerly CCITT), *Broadband Integrated Services Digital Network (B-ISDN) Asynchronous Transfer Mode (ATM) Functional Characteristics,* Recommendation I.150, 1991.

[ITU 92] International Telecommunications Union – Telecommunications Sector (formerly CCITT), *Integrated Services Digital Network (ISDN) Data Link Layer Specification for Frame Mode Bearer Services,* Recommendation Q.922, 1992.

[JSC 94] Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence,* February 28, 1994.

Appendix E – References (continued)

[KIRKPAT 91] K. E. Kirkpatrick, "OSI-Based LAN Security Standards," *Handbook of Local Area Networks,* Auerbach Publications, Boston Massachusetts, 1991, pp. 741-753

[MISSI 93A] MISSI Program Office (NSA), *MISSI System Architecture, FOUO,* March 17, 1993.

[MISSI 93B] MISSI Program Office (NSA), *System Security Framework for the Multilevel Information System Security Initiative (MISSI), FOUO,* Draft, April 20, 1993.

[MISSI 93C] MISSI Program Office (NSA), *Multilevel Information Systems Security Program, FOUO,* August 3, 1993.

[MISSI 94] MISSI Program Office (NSA), *Multilevel Information Systems Security Initiative (MISSI) Network Security Managers (NSM) Functional Requirements Specification and Concept of Operations (CONOP) Version 3.2, FOUO,* Draft, February 3, 1994.

[NAVSEA 93] Naval Sea Systems Command, *Integrated Interior Communications and Control (IC)2 Program Plan,* circa August 18, 1993.

[NIST 90A] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols,* NISTIR 90-4250, February 1990.

[NIST 90B] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Access Control Documents,* NISTIR 90-4259, February 1990.

[NIST 90C] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Key Management Documents,* NISTIR 90-4262, February 1990.

[NIST 91] National Institute of Standards and Technology, *Government Open Systems Interconnection Profile (GOSIP),* FIPS PUB 146-1, April 1991.

[NIST 93] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Message Security Protocol (MSP),* SDN.701, Revision 2.1, November 23 1993.

[NRaD 92] Naval Command, Control, and Ocean Surveillance Center (NCCOSC) Research, Development, Test, and Evaluation (RDTE) Division, *An Encryption Peripheral for Application Level Service,* August 11, 1992.

Appendix E – References (continued)

[NRaD 94A] Naval Command, Control, and Ocean Surveillance Center (NCCOSC) Research, Development, Test, and Evaluation (RDTE) Division, *Command and Control Warfare Distributed Multilevel Security – INFOSEC for the C4I Warrior, V.1.7,* March 22, 1994.

[NRaD 94B] Naval Command, Control, and Ocean Surveillance Center (NCCOSC) Research, Development, Test, and Evaluation (RDTE) Division, *ALLPOWER The ALL PurpOse Workstation sEcurity peRipheral,* April 11, 1994.

[NRL 92] Naval Research Laboratory, *Multi-Level Secure (MLS) Processing System 6.3A Core Technology Program Execution Plan,* October 2, 1992.

[NRL 93A] Naval Research Laboratory, *User Level Security in the Copernicus TADIXS, Technical Memorandum 5520-36A,* March 26, 1993.

[NRL 93B] Naval Research Laboratory, *Information Security in the Copernicus Architecture,* NRL briefing to NSA on Copernicus and Programmable Embeddable INFOSEC Product, May 20, 1993.

[NSA 93A] National Security Agency, *DoD Information Systems Security Policy, DISSP-SP.1,* February 22, 1993.

[NSA 93B] National Security Agency, *MOSAIC Key Management Concept, Revision 2.4,* August 18, 1993.

[NSA 94] National Security Agency, *MOSAIC Program Overview, Version 2,* January 28, 1994.

[NSTISSI 92] National Security and Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, *National Information System Security (INFOSEC) Glossary,* June 5, 1992.

[RFC 80] Internet Network Working Group, *User Datagram Protocol,* J. Postel, Request for Comments: 0768, STD 6, August 28, 1980.

[RFC 81A] Internet Network Working Group, *Transmission Control Protocol,* J. Postel, Request for Comments: 0793 (updates RFC 0761), STD 7, September 1, 1981.

[RFC 81B] Internet Network Working Group, *Internet Protocol,* J. Postel, Request for Comments: 0791 (obsoletes RFC 0760), September 1, 1981.

Appendix E – References (continued)

[RFC 82] Internet Network Working Group, *Simple Mail Transfer Protocol,* J. Postel, Request for Comments: 0821 (obsoletes RFC 0788), STD 10, August 1, 1982.

[RFC 83] Internet Network Working Group, *Telnet Protocol Specification,* J. Postel and J. Reynolds, Request for Comments: 0854 (obsoletes RFC 0764), STD 8, May 1, 1983.

[RFC 85] Internet Network Working Group, *File Transfer Protocol,* J. Postel and J. Reynolds, Request for Comments: 0959 (obsoletes RFC 0765), STD 9, October 1, 1985.

[RFC 89] Internet Network Working Group, *Simple Network Management Protocol SNMP,* J. Case, C. Davin, and M. Fedor, Request for Comments: 1098 (obsoletes RFC 1067) (updated by RFC 1157), April 1, 1989.

[RFC 90] Internet Network Working Group, *A Simple Network Management Protocol (SNMP),* J. Postel, Request for Comments: 1157 (updates RFC 1098), STD 15, May 10, 1990.

[RFC 93A] Internet Network Working Group, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2),* J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Request for Comments: 1448, May 3, 1993.

[RFC 93B] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures,* J. Linn, Request for Comments: 1421 (obsoletes RFC 1113), February 1993.

[SCHNEIER 94] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* John Wiley and Sons, New York, 1994.

[SKIPJACK 93] E.F. Brickell, et al., *SKIPJACK Review Interim Report: The SKIPJACK Algorithm,* New York, 1993.

[SPAWAR 91A] Chief of Naval Operations, Space and Naval Warfare Systems Command, Copernicus Project Office, *The Copernicus Architecture – Phase I: Requirements Definition,* August 1991.

[SPAWAR 91B] Chief of Naval Operations, Space and Naval Warfare Systems Command, Copernicus Project Office, *The Copernicus Architecture – Initial Implementation Plan for Phase II,* December 1991.

Appendix E – References (continued)

[SPAWAR 92A] Chief of Naval Operations, Space and Naval Warfare Systems Command, Copernicus Project Office, *Security Policy for the Copernicus TADIXS,* December 21, 1992.

[SPAWAR 92B] Space and Naval Warfare Systems Command, *Embeddable INFOSEC Product Security Placement Options,* August 21, 1992.

[SPAWAR 94] Chief of Naval Operations, Space and Naval Warfare Systems Command, Information Systems Security Office, CDR Dan Galik, *Navy INFOSEC – Multilevel Security (MLS),* briefing slides, circa January 1994.

[SSI 92] Secure Solutions, Inc., *Placement of Network Security Services for Secure Data Exchange,* SBIR Topic N91-061, November 2, 1992.

[SSI 94A] Secure Solutions, Inc., *Technical Report – Naval Security Standards and Applications Analysis,* SBIR Topic N91-061, February 14, 1994.

[SSI 94B] Secure Solutions, Inc., *Technical Report – Analysis of End-to-End Encryption and Traffic Flow Confidentiality Options,* SBIR Topic N91-061, April 20, 1994.

[STALLING 85] W. Stallings, *Handbook of Computer Communications Standards – Local Network Standards, Volume 2,* Macmillan Publishers.

[TAYLOR 93] Michael Taylor, Digital Equipment Corporation, "Implementing Privacy Enhanced Mail on VMS," *Proceedings of the Privacy and Security Research Group Workshop on Network and Distributed System Security,* San Diego: Internet Society, February 1993, pp. 63-68.

[TIS 93] Trusted Information Systems, *Preliminary Discussion: Security Issues of a Unix PEM Implementation,* undated (circa February 1993).

[ZIMMER 92] Phil Zimmermann, *PGP User's Guide,* (Pretty Good Privacy), December 4, 1992.