

2

NAVAL POSTGRADUATE SCHOOL Monterey, California

AD-A257 327



DTIC
ELECTE
NOV 23 1992
S C D

THESIS

RISK ASSESSMENT
OF
LAN COMMUNICATIONS

by

Mark A. Paylor

September 1992

Thesis Advisor

William J. Haga

92-29914

Approved for public release; distribution is unlimited.

Unclassified

Security Classification of this page

REPORTS DOCUMENTATION PAGE

1a Report Security Classification Unclassified		1b Restrictive Markings	
2a Security Classification Authority		3 Distribution Availability of Report Approved for public release; distribution is unlimited	
2b Declassification/Downgrading Schedule		5 Monitoring Organization Report Number(s)	
6a Name of Performing Organization Naval Postgraduate School	6b Office Symbol (If Applicable) 37	7a Name of Monitoring Organization Naval Postgraduate School	
6c Address (city, state, and ZIP code) Monterey, CA 93943-5000		7b Address (city, state, and ZIP code) Monterey, CA 93943-5000	
8a Name of Funding/Sponsoring Organization	8b Office Symbol (If Applicable)	9 Procurement Instrument Identification Number	
8c Address (city, state, and ZIP code)		10 Source of Funding Numbers	
Program Element Number	Project No.	Task	Work Unit Accession No.
11 Title (Include Security Classification) Risk Assessment of LAN Communications			
12 Personal Author(s) Paylor, Mark Alan			
13a Type of Report Master's Thesis	13b Time Covered From To	14 Date of Report (year, month, day) September 1992	15 Page count 81
16 Supplementary Notation The view expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the US Government.			
17 Cost Codes:	Field	Group	Subgroup
18 Subject Terms (continue on reverse if necessary and identify by block number) Computer Security, Risk Assessment, Local Area Network			
19 Abstract (continue on reverse if necessary and identify by block number) The National Computer Security Center's (NCSC) <i>Computer Security Requirements -- Guidance for Applying the DoD TCSEC in Specific Environments</i> (CSC-STD-003-85) describes an environmental evaluation process which can be utilized to determine the level of trust required in a given Local Area Network (LAN) system for processing sensitive information. This thesis investigates the environmental evaluation process and applies it to the LAN environment of a hypothetical naval aviation squadron.			
20 Distribution/Availability of Abstract <input checked="" type="checkbox"/> unclassified/unlimited <input type="checkbox"/> same as report <input type="checkbox"/> DTIC users		21 Abstract Security Classification Unclassified	
22a Name of Responsible Individual Professor William J. Haga		22b Telephone (Include Area Code) (408) 646-3094	22c Office Symbol AS/HG

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted

Security Classification of this Page

All other editions are obsolete

Unclassified

Approved for public release; distribution is unlimited.

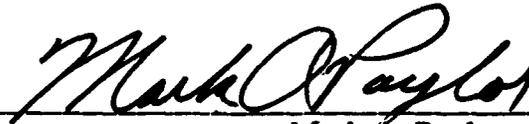
Risk Assessment of LAN Communications

by

Mark Alan Paylor
Lieutenant Commander, United States Navy
B.S., Central Washington University, 1980

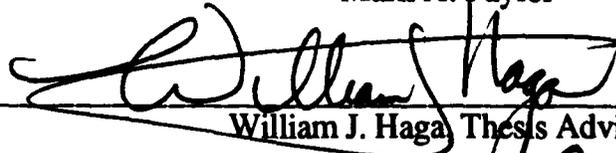
Submitted in partial fulfillment of the requirements for
the degree of
MASTER OF SCIENCE IN INFORMATION SYSTEMS
from the
NAVAL POSTGRADUATE SCHOOL
September 1992

Author:

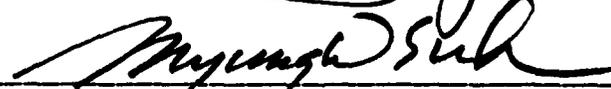


Mark A. Paylor

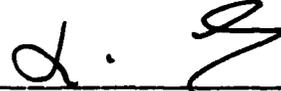
Approved by:



William J. Haga, Thesis Advisor



Myung W. Suh, Second Reader



David Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

The National Computer Security Center's (NCSC) *Computer Security Requirements -- Guidance for Applying the DoD TCSEC in Specific Environments* (CSC-STD-003-85) describes an environmental evaluation process which can be utilized to determine the level of trust required in a given Local Area Network (LAN) system for processing sensitive information. This thesis investigates the environmental evaluation process and applies it to the LAN environment of a hypothetical naval aviation squadron.

DTIC QUALITY INSPECTED 4

Accession For	
NTIS GRAND	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

TABLE OF CONTENTS

I.	INTRODUCTION	1
A.	BACKGROUND	1
B.	PROBLEM.....	2
C.	OBJECTIVE.....	2
II.	COMPUTER SECURITY: A HISTORICAL PERSPECTIVE	3
III.	STANDARD FOR TRUSTED SYSTEMS	7
A.	THE ORANGE BOOK.....	7
1.	The Criteria - A Security Evaluation Metric	7
2.	Control Objectives	9
B.	PROBLEMS WITH THE ORANGE BOOK.....	10
IV.	GUIDELINES FOR NETWORK SECURITY.....	14
A.	TRUSTED NETWORK TECHNOLOGY (TNT) PUBLICATIONS	14
1.	Trusted Network Interpretation (TNI).....	14
2.	Trusted Network Interpretation Environments Guidelines (TNIEG).....	15
B.	RISK ASSESSMENT - A METHODOLOGY FOR RISK MANAGEMENT.....	15
1.	Risk Analysis.....	16
2.	Risk Assessment	17
V.	NETWORK RISK ASSESSMENT	19
A.	TNI PART I SECURITY REQUIREMENTS	19
B.	TNI PART II SECURITY REQUIREMENTS.....	21
1.	Determination of Part II Risk	24
2.	Strength of Mechanism Requirement.....	26
3.	Assurance Requirement.....	27

4. Functionality Requirement.....	29
VI NETWORK RISK ASSESSMENT: A CASE STUDY	30
A. BACKGROUND	30
B. TACAMO LAN	32
C. ADP OFFICER PLAN OF ATTACK	33
D. PHASE I - TNI PART I RISK ASSESSMENT OF VQ-7	34
1. Step 1: Determine system security mode of operation.	34
2. Step 2: Determine minimum user clearance or authorization rating.	34
3. Step 3: Determine maximum data sensitivity rating.....	35
4. Step 4: Determine risk index.....	35
5. Step 5: Determine minimum security evaluation class for computer-based controls.....	35
6. Step 6: Determine <i>adjustments</i> to computer security evaluation class required.....	36
E. PHASE I - TNI PART II RISK ASSESSMENT OF VQ-7.....	36
1. Functionality.....	36
2. Strength of Mechanism.....	36
3. Assurance	37
4. Part II Assurance Rating versus Minimum Part I Evaluation.....	37
VII. NETWORK RISK ASSESSMENT: ANALYSIS AND CONCLUSIONS	39
A. OVERVIEW OF FINDINGS.....	39
B. COMMENTS ON THE RISK ASSESSMENT PROCESS.....	42
C. DIRECTIONS FOR FUTURE RESEARCH.....	44

1. Phase II - Identify, procure, and implement "trusted products"	44
2. Phase III - Certification and accreditation (C & A) of trusted systems	45
D. FINAL REMARKS	46
APPENDIX A	48
APPENDIX B	49
APPENDIX C	50
A. FEDERAL REGULATIONS	50
B. DEPARTMENT OF DEFENSE SECURITY POLICY	50
C. SECURITY STANDARDS	51
APPENDIX D	52
A. CLEARANCES	52
B. DATA SENSITIVITIES	53
APPENDIX E	55
APPENDIX F	57
APPENDIX G	58
A. AUTHENTICATION	58
B. COMMUNICATIONS FIELD INTEGRITY	60
C. NON-REPUDIATION	61
D. DENIAL OF SERVICE	61
E. PROTOCOL BASED DOS PROTECTION	62
F. NETWORK MANAGEMENT	63
G. DATA CONFIDENTIALITY	64
H. TRAFFIC FLOW CONFIDENTIALITY	64
I. SELECTIVE ROUTING	64

APPENDIX H.....	65
APPENDIX I.....	66
A. AUTHENTICATION.....	66
B. COMMUNICATIONS FIELD INTEGRITY.....	66
C. NON-REPUDIATION.....	67
D. DENIAL OF SERVICE.....	67
E. PROTOCOL BASED DOS PROTECTION.....	68
F. NETWORK MANAGEMENT.....	68
G. DATA CONFIDENTIALITY.....	68
H. TRAFFIC FLOW CONFIDENTIALITY.....	69
I. SELECTIVE ROUTING.....	69
LIST OF REFERENCES.....	70
INITIAL DISTRIBUTION LIST.....	72

ACKNOWLEDGMENT

This thesis is dedicated to my wife Laura and my children Nicole and Christopher. Their support and patience made this research effort an enjoyable experience.

I. INTRODUCTION

A. BACKGROUND

The United States Navy entered the office automation (OA) systems age in the 1980's and now, in the 1990's, looks forward to anticipated benefits from newer technologies. The Navy's aviation squadrons are currently using stand alone microcomputers in their work place. Since their introduction in the 1980's, these microcomputers, or OA systems, have improved the capability and effectiveness of the operational units that employ them. These systems "have generally increased the productivity of the administrative personnel by allowing each (person) to produce more information of a higher quality than was previously possible in a manual mode." (McMican, 1985) New computer technologies are now promising even greater improvements in administrative productivity and efficiency. The local area network (LAN) is one of these new technologies.

The Navy has already begun to plan and implement LAN technology in its organizational units. Many of the Navy's ships already have networks installed and new ships, such as the aircraft carrier GEORGE WASHINGTON, are now being designed to incorporate them from the start. Another example of LAN technology implementation is the Naval Aviation Logistics Command Management Information System (NALCOMIS). This system is designed to automate the Naval Aviation Maintenance Program (NAMP) business functions and to implement a standardized management system. Planning for the implementation of LANs in aviation squadrons is also underway. "COMNAVAIRPAC has plans to provide funding for LANs at the squadron level in the coming years." (Shannon, 1992)

B. PROBLEM

COMNAVAIRPAC has identified the need for their squadron LANs to handle multiple levels of classified information up to but not greater than secret. The design and implementation of such a LAN raises several questions. What security issues should be considered in the design phase of a LAN with this requirement? What Department of Defense (DoD) directives and National Computer Security Center (NCSC) guidelines must be adhered to? How is the level of trust required for a particular LAN determined? How is a LAN certified and accredited to operate at a particular level of trust?

C. OBJECTIVE

The National Computer Security Center (NCSC) provides guidance on security in networks through the Trusted Network Technology (TNT) publications. The TNT includes the Trusted Network Interpretation (TNI) and the Trusted Network Interpretation Environments Guideline (TNIEG). For now, the TNT publications provide the only guidance available.

The objective of this thesis is to survey the TNT publications, focusing on the risk management methodologies that they describe. Specifically, the risk assessment methodology used to determine the minimum security requirements for a network will be analyzed in detail and applied to a hypothetical aviation squadron. The results of this application will be summarized and used as the basis for trusted network design recommendations.

Background information on networks and security can be obtained from the recommended readings listed in Appendix A.

II. COMPUTER SECURITY: A HISTORICAL PERSPECTIVE

Computer security is not a new issue. Early computer security activities date back to the 1950's with the development of the first TEMPEST¹ standard and the establishment of the U.S. Communications Security (COMSEC) Board. Government and industry had become concerned about the possibility of compromising classified information by electronic eavesdropping. "Studies of signal interception and decoding have borne out these speculations." (Russell and Gangemi, 1991) It was not until the 1960's, however, that computer security received recognition as a serious issue. A Joint Computer Conference was held in the Spring of 1967 and is considered one of the first comprehensive computer security presentations. It covered a variety of threats ranging from electromagnetic radiation to unauthorized programmer and user access to systems and data. This presentation, however, was merely an introduction to the possible vulnerabilities and did not include discussions on how to counter these threats. (Russell and Gangemi, 1991)

In 1967, the Defense Science Board sponsored the establishment of a task force within the Advanced Research Projects Agency (ARPA) that began an examination of computer system and network vulnerabilities. The task force was to examine, identify and introduce methods for protecting and controlling access to the government computer systems and information. The task force published a report after two years of study called Security Controls for Computer Systems. This report is considered to be a significant publication in the history of computer security. "Its recommendations, and the research that followed its publication, led

¹TEMPEST refers to the U.S. government program established to combat the electromagnetic emanations problem. It also refers to technology that contains or suppresses signal emanations from electronic equipment. (Russell and Gangemi, 1991)

to a number of programs dedicated to protecting classified information and setting standards for protection." (Russell and Gangemi, 1991) The recommendations of this report also led to DoD's development of regulations for enforcing security of computer systems, networks, and data processed by DoD.

In 1972, DoD established a policy for computer controls and techniques titled Security Requirements for Automatic Data Processing (ADP) Systems (DoD Directive 5200.28). This directive mandated the protection of both computer system equipment and data from unauthorized access and manipulation.

DoD continued its computer security efforts in the 1970's by sponsoring initiatives in three categories: tiger teams, security research studies, and development of the first secure operating systems. Tiger teams were used to detect and attempt to fix computer security problems. They were of limited use since one tiger team often found flaws that another tiger team had missed previously.

The security research studies resulted in a couple of important concepts. One concept was a reference monitor, an entity that "enforces the authorized access relationships between subjects and objects of a system." (Anderson, 1972; Russell and Gangemi 1991) A subject is a person, process or device that causes information flow among objects. An object is a passive entity that contains or receives information such as files, directories, programs and printers. This concept was used in the development of standards and technologies for secure systems. Another important concept was the development of security policy models. This concept has two parts, the security policy and the security model. The security policy is a set of laws, rules and practices that regulate the management, protection, and distribution of sensitive information. The security model refers to the mechanisms required to enforce the security policy. Bell and LaPadula [1976]

were the first to develop a mathematical model of a multi-level security policy. This model "was central to the development of basic computer security standards and laid the groundwork for a number of later security models, and their application in government security standards." (Russell and Gangemi, 1991)

Much of the secure systems development research conducted in the 1970's focused on working models of security kernels. This concept involves building the operating system with a portion (kernel) devoted to controlling the access to system resources. One of the successful developments using this concept was the Multics (Multiplexed Information Computing Service) system funded by the Air Force. Its well designed security features provided a model example for the development of the secure systems that followed.

In the late 1970's, both DoD and the National Bureau of Standards (NBS) (now NIST) organized a number of seminars and invitational workshops involving government and industry experts in computer technology and security. The DoD seminars focused on answering the following questions. "Are secure computer systems useful and feasible? What mechanisms should be developed to evaluate and approve secure computer systems? How can computer vendors be encouraged to develop secure computer systems?" (Russell and Gangemi, 1991) This initiative by DoD was known as the DoD Computer Security Initiative and its goal was to bring attention to computer security issues. This initiative was successful in that the attention it received led to a second important initiative from NBS. A series of NBS Invitational Workshops made significant progress toward the development of standards for secure systems. The attending computer experts reported that they identified three areas that required specific attention to achieve security. (1) Policy: What security rules should be enforced for sensitive information?; (2) Mechanisms: What hardware and software

mechanisms are needed to enforce the policy?; and (3) Assurance: What needs to be done to make a convincing case that the mechanisms do support the policy even when the system is subject to threats?

Once the questions had been asked, the task of answering them had to be assigned. The Mitre Corporation was tasked with the development of the first set of computer security evaluation criteria for the use of assessing the degree of trust that could be placed in a computer system that protected classified data. The Invitational Workshops also led to follow-on public seminars conducted by the Office of the Secretary of Defense concerning the DoD Computer Security Initiative. As a result, the National Security Agency (NSA) received new responsibility for information security and established the DoD Computer Security Center (CSC) within NSA in 1981. Its basic charter was to continue and expand upon the work started by the DoD Computer Security Initiative. Four years later, the CSC's name was changed to the National Computer Security Center (NCSC) when its responsibilities for computer security expanded to include all federal agencies. Appendix B contains a listing of the NCSC's goals. (Russell and Gangemi, 1991)

III. STANDARD FOR TRUSTED SYSTEMS

A. THE ORANGE BOOK

The NCSC's charter to continue the work started by the DoD Computer Security Initiative and the MITRE Corporation led to the development of evaluation criteria that could be used to quantify computer security. These criteria were published in the DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)*. The Orange Book, as it is commonly referred to because of its color, became the bible of secure computer system development.

1. The Criteria - A Security Evaluation Metric

The Orange Book defines the criteria used to classify systems based on the level of trust that can be placed in a computer system. The criteria were developed to (1) provide guidance to manufacturers as to what to build into their computer security products, (2) provide computer users with a metric for determining the level of trust that can be placed in systems that process classified or other sensitive information and (3) provide a standard that can be followed in computer product acquisition specifications. (DoD, 1985)

The TCSEC specifies a "secure" computing system as one that will control access to information, such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create or delete information. There are four major divisions of criteria that are structured in a hierarchical fashion: D, C, B and A. Division A identifies systems with the most stringent protection and division D identifies those systems that have been evaluated and found to offer unacceptable security protection.

Division A provides the most comprehensive security protection (Verified Protection). However, it is difficult to implement and difficult to evaluate. The definition of division A follows.

Division A requires the use of formal security methods to assure that the mandatory and discretionary security controls, employed in the network system, can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the NTCB (Network Trusted Computing Base) meets the security requirements in all aspects of design, development, and implementation. (NCSC, 1987)

Division B (Mandatory Protection) requires more stringent controls and testing than Division C but is easier to develop and evaluate than Division A. Division B is based on the integrity of required sensitivity labels. It uses sensitivity labels to enforce a set of "mandatory" access control rules (NCSC, 1987). The sensitivity labels must be carried with all information in the network.

Division B contains three classes (B1, B2, and B3). Class B1 requires the features specified at its division level. Class B2 and B3 require more stringent controls and move beyond the basic requirements toward the requirements of division A.

Division C provides discretionary (need-to-know) protection, identification/authentication capabilities, and accountability of subjects (users/processes started by them) and the actions they initiate via audit capabilities. Audit capabilities are used to track a subject's use or modification of an object, providing a means of holding users (subjects) accountable for their actions. Class C1 requires the features of Division C but does not require an audit trail. Class C2 enforces a more stringent discretionary access control (DAC) than C1 by requiring auditing of security-relevant events and resource encapsulation. (DoD, 1985)

Division D is reserved for those systems or LAN's that do not meet one of the preceding divisions and is considered to provide only minimal protection.

2. Control Objectives

In addition to the seven criteria described above, general control objectives were developed to give guidance in designing trusted computer systems. The control objectives are security policy, accountability, assurance and documentation.

Security policy is a statement of intent that specifies the control to be used for access and dissemination of sensitive information. Accountability refers to the ability of the system to assure individual accountability based on the type of security policy invoked. Assurance refers to the systems ability to ensure accurate interpretation of the security policy during operation and throughout the system's life-cycle. Documentation refers to user guides, manuals and other written documents that support each class.

Each control objective described above is made up of a group of requirements. "These groupings were developed to assure that (these) control objectives for computer security are satisfied and not overlooked" (DoD, 1985). The Orange Book contains a more detailed discussion of the control objectives and their requirements.

Table 1 shows the relationship between the Orange Book evaluation criteria and the control objectives for trusted computer systems. It depicts the changes in requirements between each class.

TABLE 1
TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
SUMMARY CHART

	C1	C2	B1	B2	B3	A1	
Discretionary Access Control							Security Policy
Object Reuse							
Labels							
Label Integrity							
Exportation of Labeled Information							
Exportation of Multilevel Devices							
Exportation of Single-Level Devices							
Labeling Human-Readable Output							
Mandatory Access Control							
Subject Sensitivity Labels							
Device Labels							
Identification and Authentication							Accountability
Audit							
Trusted Path							
System Architecture							Assurance
System Integrity							
Security Testing							
Design Specification and Verification							
Covert Channel Analysis							
Trusted Facility Management							
Configuration Management							
Trusted Recovery							
Trusted Distribution							
Security Features User's Guide							Documentation
Trusted Facility Manual							
Test Documentation							
Design Documentation							

- No requirements for this class
- New or enhanced requirements for this class
- No additional requirements for this class

(Russell and Gangemi, 1991; DoD, 1985)

B. PROBLEMS WITH THE ORANGE BOOK

Russell and Gangemi [1991] have identified a few of the major claims against the Orange Book by some respected security practitioners. The cited Orange

Book inadequacies are: the Orange Book model targets the government classified environment only versus the commercial environment; the Orange Book's narrow focus on only one security principle - secrecy; the Orange Book emphasis on unauthorized access protection from external intruders versus the possibility of intrusion from insiders; the Orange Book's failure to address network issues; and the Orange Book's failure to offer more than just a few, limited security ratings.

When the Orange Book (TCSEC) was issued in 1985, its objective was, and still is, to "provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products." (DoD, 1985) It was not intended to be a comprehensive document that addresses all computer security issues. Although the TCSEC was designed to be application-independent, the NCSC recognized that the security requirements specified by the criteria would eventually have to be adapted or expanded in order to apply them to other types of computer systems (i.e., networks and data bases), each having their own functional requirements or special environments. The TCSEC criteria and technical evaluation methodologies provide an important reference foundation for new computer technologies. Improvements to the Orange Book criteria and their methodologies have been identified and further research and debate are being solicited via technical reports. (NCSC, 1991)

The NCSC designed and implemented Technical Guidelines Program to ensure that the features of the TCSEC are discussed in detail and that guidance is provided for meeting the different requirements of evolving computer technologies. This program has resulted in over 20 publications that have become collectively known as the Rainbow Series because of the different colors used for their covers. Many of these technical guidelines have addressed the

Orange Book shortcomings mentioned earlier. However, others have yet to be addressed in future revisions of the Orange Book.

Although the Orange Book provides a mechanism to make revisions through a formal review process, no revisions have been made since its original issue in 1985. So far, the only evidence of a revision to the Orange Book is an NCSC technical report, *Integrity-oriented Control Objectives: Proposed Revisions to the Trusted Computer System Evaluation Criteria (TCSEC)*, published in October of 1991. This technical report has been issued as a proposed change to a specific section of the Orange Book, namely, the control objectives. "This document proposes new and revised versions of the control objectives and (is) intended to be used as a strawman to foster further research and debate aimed at developing a new or revised set of product evaluation criteria that addresses integrity as well as confidentiality" (NCSC, 1991). Although this technical report focuses on only one aspect of the Orange Book criteria (control objectives) it does state that further research and debate is needed before the proposal is adopted. It is not clear, however, how long this process will take and what affect each specific revision will have individually or as a whole on the updating of the Orange Book.

Tannis [1988] cites the technical guidelines development process itself as another shortcoming. The NCSC originally implemented its Technical Guidelines Program with a policy that dictated guideline production in a serial manner and was based on the perceived urgency of addressing specific computer security issues. Addressing the many areas of information security (INFOSEC) in a serial manner did not, however, meet the ever growing demands for guidance in the application of new computer technologies. As a result, the NCSC adopted a new policy that dictated the use of its resources in concurrent efforts. This new policy

of concurrent guidelines development, however, is the root of a shortcoming in the technical guidelines development process.

Concurrent development of technical guidelines does not provide for collaboration between different groups of Technical Guidelines Division personnel conducting individual research on separate security issues. Since many of the computer security issues being addressed by the Technical Guidelines Program are closely inter-related, there may be duplication of effort. Additionally, without a concerted effort by the Technical Guidelines Division personnel on these inter-related issues, it may be difficult to produce guidelines that consider all aspects of a particular security issue and minimize redundant efforts. Unfortunately, the Technical Guidelines Program addresses only one computer security issue per effort and does not provide a means for collaboration. Since each security issue to be researched is isolated from other inter-related issues, the real-world affects of one issue versus many others is lacking in the guideline that results. (Tannis, 1988)

IV. GUIDELINES FOR NETWORK SECURITY

A. TRUSTED NETWORK TECHNOLOGY (TNT) PUBLICATIONS

The NCSC's ongoing research and invitational workshops led to the drafting of the Trusted Network Technology (TNT) publications. These technical publications were developed to provide guidance on how new security technology should be used. The first of these publications was the Trusted Network Interpretation (TNI) of the TCSEC. The TNI was issued as an addition to the Rainbow Series in 1987 and added "interpretation and rationale to applying trust technology to network systems." (NCSC, 1990) The second of these publications was the Trusted Network Interpretation Environments Guideline (TNI EG) issued in 1990. The TNI EG provides guidance on the use of the TNI. It helps to identify the security protection required in different network environments.

The TNI and TNI EG do not cover all of the necessary security requirements that should be considered in a trusted network. They provide "the best guidance that is available at this time." As technology continues to advance and research produces improved computer security methodologies, additional guidance will be provided. (NCSC, 1990)

1. Trusted Network Interpretation (TNI)

The TNI was written to serve the same purpose for networked systems that the TCSEC does for general purpose computers. Essentially, it extends the classes and criteria to trusted network systems and components. The document is divided into two parts. Part I provides interpretations of TCSEC security features and assurance requirements. Its evaluation system is identical to that of TCSEC (Arsenault, 1987). Part II of the TNI describes additional security services (e.g.,

communications integrity, denial of service, transmission security) that are of significant concern in the network environment. (NCSC, 1987)

2. Trusted Network Interpretation Environments Guidelines (TNIEG)

In 1990, the Trusted Network Interpretation Environments Guideline (TNIEG) was issued to provide "insight into the issues relevant when integrating, operating, and maintaining trusted computer networks" (NCSC, 1990). Specifically, the TNIEG describes many issues that can arise when determining security requirements in different network environments. As stated earlier, the TNIEG does not address all of the possible security protection issues but is considered "the first step" toward identifying the minimum security protection required in different environments. (NCSC, 1990)

B. RISK ASSESSMENT - A METHODOLOGY FOR RISK MANAGEMENT

Computer security requirements are addressed in several federal regulations, policies, and standards. Appendix C contains an overview of these documents. The overall computer security policy document for the Department of Defense is DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs). It provides guidance on mandatory and minimum AIS security requirements.

DoD Directive 5200.28 mandates that a risk management program be used for the management of DoD computer systems. DoD Directive 5200.28 [1988] defines risk management as follows:

The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.

The risk analysis mentioned in the definition above refers to a methodology that analyzes AIS "assets and (their) vulnerabilities to establish an expected loss

from certain events based on estimated probabilities of occurrence" (DoD, 1988). It involves a series of steps that (1) identifies the exposures of an AIS, (2) identifies possible controls and their costs for each exposure, and (3) analyzes the cost and benefit of protecting the AIS from the identified exposures. This risk analysis methodology, however, differs from the risk assessment methodology described in the TNIEG (and mandated by DoD Directive 5200.28),

Risk assessment refers to the determination of "the recommended (NCSC) evaluation class (or requirements of an evaluation class) based on a specific environment" (NCSC, 1990). The environment that it evaluates is characterized by (1) AIS users possessing different security clearances, and (2) the data processed on the AIS having different levels of data sensitivity. The risk assessment methodology compares the environmental factors to determine which NCSC evaluation rating will provide the necessary security for the AIS. Appendix D describes user clearances and data sensitivities in detail.

This thesis focuses on the risk assessment methodology and will not address the other elements of risk management. A brief discussion of risk analysis and risk assessment is provided below.

1. Risk Analysis

The risk analysis of computer systems is a sub-task of risk management and is used to establish an overall computer system security policy. Security planning begins with risk analysis to determine all exposures of a computing system and the costs of controlling each exposure. A cost-benefit analysis of this information provides quantifiable answers to questions regarding the cost of a control versus the cost of asset loss. Several benefits can result from a traditional risk analysis: (1) improved employee awareness; (2) identification of computing

assets, vulnerabilities, and controls; (3) improved basis for risk versus control decisions; (4) a means of justifying expenditures for security. (Pfleeger, 1989)

Risk analysis helps to determine how important the computer system is and how far the organization is willing to go (concerning equipment, people, and budget) to protect it. The risk analysis is typically structured to: (1) determine an organizations assets (people, software, hardware and procedures); (2) assess the nature and size of asset vulnerability to the five main threats (destruction, modification, disclosure, denial and fraud); (3) estimate the probability of the threat occurring; (4) estimate the single loss from the threat occurring; (5) estimate the annualized loss expectancy; (6) devise effective controls or safeguards; (7) establish a cost-benefit analysis; and (8) select the most cost effective alternatives. (Russell and Gangemi, 1991)

2. Risk Assessment

In computer security, the government's most valuable asset is probably the information that is processed on its computers. There are many security requirements to be considered. "Depending on the particular environment, communications security (COMSEC), emanations security (TEMPEST), physical security, personnel security, administrative security, and other information security (INFOSEC) measures or safeguards are ... required" (NCSC, 1990).

Enclosure (4) of DoD Directive 5200.28 describes risk assessment as a procedure that leads to the selection of security services and safeguards that are appropriate for a given network environment. The risk assessment methodology compares user clearances and data sensitivities using a series of tables. The results of the assessment help determine the minimum level of trust recommended for a specific network environment. The TNIEG relies heavily on this risk assessment methodology and will provide the basis for its description and

application. The details of this environmental risk assessment process will be described in the chapters that follow.

V. NETWORK RISK ASSESSMENT

A. TNI PART I SECURITY REQUIREMENTS

The TNIEG describes a procedure that uses the highest classification of data and the lowest clearance among system users to compute an overall risk index. Once computed, the risk index is used to determine the corresponding NCSC-evaluation rating (TCSEC criteria) required for the system to provide adequate security.

As discussed earlier, Enclosure (4) of DoD Directive 5200.28 describes risk assessment in detail. It describes six major steps in assessing risk: (1) determine system security mode of operation; (2) determine minimum user clearance or authorization rating; (3) determine maximum data sensitivity rating; (4) determine risk index; (5) determine minimum security evaluation class for computer-based controls; and (6) determine adjustments to computer security evaluation class required. (NCSC, 1987)

The TNIEG uses adaptations from DoD Directive 5200.28 (Enclosure 4) to illustrate the steps to be followed in determining the risk of a network. The first step requires the selection of the desired system security mode of operation (Appendix F). The second step describes the determination of the minimum clearance or authorization of the network users. Appendix D contains a detailed description of user clearances. Once this is determined, Table 2 is used to assign a rating for the minimum user clearance (R_{min}).

TABLE 2
RATING SCALE FOR MINIMUM USER CLEARANCE (R_{min})

Minimum User Clearance	R _{min}
Uncleared OR Not Authorized (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS) and/or current Background Investigation (BI)	4
TS and/or current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

(NCSC, 1990)

The third step describes the determination of the maximum sensitivity of data processed by the network. Appendix D contains a detailed description of data sensitivities. Appendix E contains all footnotes for the tables that follow. Once the data sensitivity is determined, it, too, is matched with a table. Table 3 assigns a rating for the maximum data sensitivity (R_{max}).

Using the numbers derived from the tables above, the risk index for a given network can be calculated using the following formula (NCSC, 1990): Risk Index = R_{max} - R_{min}.

The Risk Index is then matched to an additional table (Table 4) that will provide a minimum NCSC-evaluation rating and the security mode in which that minimum security class should operate for the network. Appendix F contains detailed descriptions of each security mode. (NCSC, 1990)

TABLE 3

RATING SCALE FOR MAXIMUM DATA SENSITIVITY (R_{max})

Maximum Sensitivity Ratings without Categories	Rating (R _{max})	Maximum Data Sensitivity with Categories 1,2	Rating (R _{max})
Unclassified (U)	0	N/A ³	
Not Classified but Sensitive (N) ⁴	1	N with one or more Categories	2
Confidential (C)	2	C with one or more Categories	3
Secret (S)	3	S with one or more Categories only one Category containing S	4
		S with two or more Categories containing S	5
Top Secret (TS)	5 ⁵	TS with one or more Categories only one Category containing S or TS	6
		TS with two or more Categories containing S or TS	7

TABLE 4

SECURITY RISK INDEX

Risk Index	Security Mode	Minimum Security Class ⁴
0	Dedicated ⁵	No Minimum Class ^{1,2}
0	System High	C2 ²
1	Multilevel, Partitioned	B1 ³
2	Multilevel, Partitioned	B2
3	Multilevel	B3
4	Multilevel	A1
5	Multilevel	*
6	Multilevel	*
7	Multilevel	*

(NCSC, 1990)

B. TNI PART II SECURITY REQUIREMENTS

Part II of the TNI provides a qualitative appraisal of security services in three aspects: functionality, strength of mechanism, and assurance. Functionality identifies the objective and the approach of a particular security service that

includes features, mechanism, and performance. Different applications environments may require the use of alternative approaches to achieve the desired functionality. Strength of mechanism identifies how well a particular approach may achieve its objectives. A mechanisms strength is affected by the selection of security parameters (such as the number of bits used in a checksum) and its ability to operate during inadvertent threats (such as natural disasters, operator errors, and accidents). Assurance refers to the belief that the functionality will be achieved and includes verifiability, resistance against circumvention or bypass, and tamper resistance. It is based on the use of formal or informal analysis of approaches such as validation and verification, testing, software engineering, and theory. (NCSC, 1990)

TNI Part II concerns itself with end to end threats (between hosts) on the network. Most of these threats do not occur in stand-alone computers. The services described above typically use software protocols (rules) in providing protection against these threats. Additional methods such as encryption may be utilized to guard against some of these threats, however these additional methods are not considered in this evaluation. (NCSC, 1990)

Computer technology has advanced rapidly over the last few decades. Unfortunately, computer security technology has lagged far behind. Although TNI Part I is well structured and developed, "Part II services have not been supported by equally well developed theories and detailed evaluation criteria ..." (NCSC, 1990). As a result, the evaluations of Part II have been designed to be qualitative rather than hierarchically-ordered like the ratings from the TCSEC. Table 5 shows the evaluation structure for network security services described in TNI Part II.

Each network environment is different and therefore each will have different needs and requirements for the additional security services described in the TNI Part II. The TNIEG discussion of the TNI Part II security requirements describes a guideline that management personnel can use in making the selection decision. A series of questions helps "determine whether a particular service (shown in Table 5) is required and what functionality is needed" (NCSC, 1990). Appendix G provides a list of these questions.

TABLE 5

EVALUATION STRUCTURE FOR NETWORK SECURITY SERVICES

Network Security Service	Criterion	Evaluation Range
Communications Integrity Authentication	Functionality	None present
	Strength	None - good
	Assurance	None - good
Communications Field Integrity	Functionality	None - good
	Strength	None - good
	Assurance	None - good
Non-repudiation	Functionality	None present
	Strength	None - good
	Assurance	None - good
Denial of Service Continuity of Operations	Functionality	None - good
	Strength	None - good
	Assurance	None - good
Protocol Based Protection	Functionality	None - good
	Strength	None - good
	Assurance	None - good
Network Management	Functionality	None present
	Strength	None - good
	Assurance	None - good
Compromise Protection Data Confidentiality	Functionality	None present
	Strength	Sensitivity Level
	Assurance	None - good
Traffic Flow Confidentiality	Functionality	None present
	Strength	Sensitivity Level
	Assurance	None - good
Selective Routing	Functionality	None present
	Strength	None - good
	Assurance	None - good

(Russell and Gangemi, 1991; NCSC, 1990)

1. Determination of Part II Risk

Although the security requirements in TNI Part II differ from those discussed in TNI Part I, the process for determining risk in a particular network environment is quite similar. The TNI Part II risk index is calculated using many of

the same tables in TNI Part I. Part I calculations involve the lowest cleared (AIS) user. The risk index calculation for Part II, however, concerns the clearance of outsiders (non-AIS users) that have physical access to any AIS object. As a result, each AIS device must be considered separately. "For each (AIS) object in the system, the lowest clearance of individuals with physical access to that object is used." The risk index is calculated as: Risk Index = $R_{max} - R_{min}$. Table 6, Minimum Clearance for Physical Access, is identical to Table 2. (NCSC, 1990)

TABLE 6
MINIMUM CLEARANCE FOR PHYSICAL ACCESS

Minimum User Clearance	R_{min}
Uncleared OR Not Authorized (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS) and/or current Background Investigation (BI)	4
TS and/or current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

(NCSC, 1990)

Table 7 (NCSC, 1990), Maximum Data Sensitivity is the same as Table 3 from page 21.

TABLE 7
MAXIMUM DATA SENSITIVITY

Maximum Sensitivity Ratings without Categories	Rating (Rmax)	Maximum Data Sensitivity with Categories 1,2	Rating (Rmax)
Unclassified (U)	0	N/A ³	
Not Classified but Sensitive (N) ⁴	1	N with one or more Categories	2
Confidential (C)	2	C with one or more Categories	3
Secret (S)	3	S with one or more Categories	4
		only one Category containing S S with two or more Categories containing S	5
Top Secret (TS)	5 ⁵	TS with one or more Categories	6
		only one Category containing S or TS TS with two or more Categories containing S or TS	7

2. Strength of Mechanism Requirement

Measuring the strength of mechanism involves two types of threat--inadvertent threat and malicious threat. Inadvertent threats are not applicable to this type of risk assessment. Malicious threats, however, are associated with physical access to an AIS object or to AIS transmissions. Selection of a protection mechanism is, therefore, based on the comparison and measurement of the lowest clearance of non-AIS users having physical access to AIS objects and the most sensitive information contained on the system. (NCSC, 1990)

Protection of data in a network can be provided by a combination of several mechanisms: physical, administrative, procedural, and technical. Although the TNI concerns itself with only the AIS hardware, firmware, software, and configuration management protections, different service directives and

organization regulations mandate the use of other protection mechanisms. (NCSC, 1990)

Table 8 (NCSC, 1990) now gives the strength of mechanism requirement based on the risk index.

TABLE 8
MINIMUM STRENGTH OF MECHANISM REQUIREMENT

Risk Index	Strength of Mechanism
0	None
1	Minimum
2	Fair
>2	Good

3. Assurance Requirement

Trusted computer systems rely on a Trusted Computing Base (TCB). "Similarly, trusted network systems rely on a Network Trusted Computing Base (NTCB)" (NCSC, 1990). The NTCB establishes the necessary conditions that improve the assurance of security services. It ensures that the integrity of programs is maintained and prevents unauthorized modification to objects within the network system. Access controls can be employed to isolate services that are unrelated. The access controls used are typically discretionary and mandatory access controls. The NTCB also provides the protection of the security and integrity of information assigned to the network. It ensures that the information is not weakened the by the various supporting security services. (NCSC, 1990)

Table 9 shows the association between the risk index and required assurance.

TABLE 9
MINIMUM ASSURANCE REQUIREMENTS

Risk Index	Part II Assurance Rating
0	None
1	Minimum
2	Fair
>2	Good

Assurance of Part II and Part I requirements are closely related. This is because the integrity of the services is dependent upon the protection provided by the NTCB. This dependence is shown in Table 10. (NCSC, 1990)

TABLE 10
PART II ASSURANCE RATING

Part II Assurance Rating	Minimum Part I Evaluation
Minimum	C1
Fair	C2
Good	B2

Table 10 matches the Part II assurance ratings for services to the minimum Part I evaluations that support them. It is important to note that the Minimum Part I Evaluation in Table 10 may not coincide exactly to the Evaluation Class calculated previously in Part I Table 4. Part I and Part II calculate R_{min} using different criteria. Part I determines R_{min} based on the minimum clearance or authorization of the network users. Part II determines R_{min} based on the minimum clearance of outsiders who have physical access to

network components. As a result, the particular network environment will dictate which requirement (Part I evaluation class or Part II evaluation class) will dominate.

4. Functionality Requirement

Functionality deals with determining the need or requirement for a particular security service. As mentioned earlier, the TNIEG provides a list of questions for each network security service described in TNI Part II that help identify the functionality required for each service. "The questions should be answered in sequence, unless the answer to one question contains an instruction to skip ahead." These questions are provided in Appendix G. (NCSC, 1990)

The services mentioned above are additional security considerations that arise in association with networks. They address the need for protection against compromise, denial of service, and unauthorized modification. These security services, however, may or may not be appropriate for a specific network environment. The list of questions provided in Appendix G can help management make an effective selection. (NCSC, 1990)

VI. NETWORK RISK ASSESSMENT: A CASE STUDY

A. BACKGROUND

Historically, the development and implementation of computer systems has been separate from computer security efforts. As mentioned earlier, computer security efforts still lag far behind the advancements in computer technology in general. "(Computer) security engineering and system engineering have been treated as separate disciplines with less than satisfactory results" (Pfleeger, 1992). This is due to the lack of guidance concerning the development of secure computer systems as part of the overall computer system engineering process. Although specific guidance is currently in draft form, many military activities find themselves adding security features and mechanisms to their computer systems that are already in place. For the application of this risk assessment, it is assumed that a hypothetical aviation squadron already has a LAN in place and now wants to incorporate the necessary computer security mechanisms for a trusted network.

The hypothetical aviation squadron is called Fleet Air Reconnaissance Squadron 7 (VQ-7). VQ-7 is one of only a few TACAMO² squadrons. The TACAMO project began as the concept of an airborne fleet communications broadcast system. Over the years TACAMO evolved into a communications platform serving as a command link to the fleet ballistic missile submarine force. The importance of their mission requires TACAMO squadrons to process multiple levels of classified information. Squadron (physical) security is taken seriously. The squadron spaces are considered a restricted area and are guarded by security personnel 24 hours a day. Squadron personnel have varying levels of security

² TACAMO stands for Take Charge And Move Out.

clearances (Appendix D) and are required to wear photographic identification badges that are color coded to indicate their clearance level.

VQ-7 is composed of several departments, each having a department head (see Appendix H for the VQ-7 organizational chart). As shown in Appendix H, the Automated Data Processing (ADP) officer billet is in the Special Projects Department. All billets within the squadron, including the ADP officer billet, are manned by squadron officers on a rotating basis. Billets are typically held for one year.

The ADP officer billet is difficult for the squadron to fill. There are no formal experience requirements that must be met by persons that are assigned to this billet. The Commanding Officer (CO) will usually try to find an officer within the squadron that has some experience with computers (e.g., undergraduate degree in computer science) to assign to the ADP officer billet. If there are no officers who have this type of prior experience, the CO will try to assign an officer that at least owns a personal computer and has an interest in computers beyond its basic word processing capabilities.

The current ADP officer for VQ-7 is LT Hines. Although he does not have a degree in computer science, he does have his own computer and is interested in computer technology. He has been in the job for two months.

There are other officers in the squadron with backgrounds in computer technology, however. LCDR Packard is the new assistant Operations Department officer. He has just completed the Computer Systems Management (CSM) curriculum at the Naval Postgraduate School (NPS) in Monterey, California. Although he has undergone postgraduate training in computer technology, LCDR Packard has returned to VQ-7 for his department head tour and has been assigned to a major department. This is an important milestone in an

officer's career. Other officers with experience in computer technology include the CO (a 1986 graduate of the CSM curriculum at NPS, Monterey, CA) and the Communications Department Head (a 1989 graduate of the CSM curriculum at NPS, Monterey, CA).

Department heads are routinely called upon to draft classified documents. These documents often require input from several other department heads before being editorialized and approved by the squadron CO. The current method of handling classified draft documents is to hand carry them in a labeled folder to each department head that needs to critique it. Several hours can be wasted, without prior coordination, if the drafter of the document cannot locate and receive input from the other department heads in a timely manner.

The implementation of a trusted network could improve the way classified documents are handled. A trusted network can provide department heads with the ability to electronically route classified documents to one another. Instead of hand carrying a classified document from one department head to another, the drafter of a document could send a copy of the document to each department head simultaneously. Once criticized by a department head, the document can be sent back to the drafter for correction.

B. TACAMO LAN

VQ-7 has recently relocated to Tinker Air Force Base in Oklahoma City, Oklahoma. The move for VQ-7 incorporated several improvements to its existing computing resources including the implementation of a LAN that connected all of the major squadron departments within the new hangar facility. The implementation of the LAN involved the use of VQ-7's existing desktop computers and printers. Specific computer resource descriptions are not necessary for this discussion and risk assessment.

VQ-7's CO has tasked his ADP officer (LT Hines) with studying the requirements for making VQ-7's LAN a trusted network capable of handling information from unclassified up through secret. VQ-7's mission requires frequent and simultaneous information processing at the classified levels of confidential and secret. The department heads of VQ-7 are frequently called upon to draft classified documents that require the input from other department heads and ultimately the approval by the Executive Officer (XO) and CO. The CO is interested in implementing a trusted network that will enable his department heads to draft, route for input from others, and route for his final approval via electronic means. The CO's goals are to improve the message drafting times, minimize the threat of physically misplacing classified materials, and ensure that his department heads use their time effectively and efficiently. The CO considers the implementation of a trusted network to be critical to VQ-7's mission and therefore wants it up and running in three months.

C. ADP OFFICER PLAN OF ATTACK

LT Hines is new to his job as the ADP officer and is unsure of where to begin. After soliciting help from LCDR Packard and the Communications Department head, LT Hines maps out a plan of attack for his tasking to implement a trusted network. His initial plan includes three phases: Phase I - Determine the NCSC-evaluation rating appropriate for the VQ-7 operational environment using the risk assessment described in the TNIEG; Phase II - Identify, procure, and implement the "trusted products" necessary to convert VQ-7's existing LAN into a trusted network; and Phase III - Obtain an "interim authority to operate" from the appropriate Designated Approving Authority (DAA) until formal certification and accreditation can be accomplished per DoD Directive 5200.28.

Since LT Hines is not familiar with these documents (the TNIEG, DoD Directive 5200.28), LCDR Packard explains how and where to get copies. LCDR Packard has worked with these documents and has offered to help LT Hines as much as his job would allow.

Phase I of the LT Hines plan will be described in detail. Phase II and Phase III, however, are considered to be beyond the scope of this thesis and provide areas for future research.

D. PHASE I - TNI PART I RISK ASSESSMENT OF VQ-7

After obtaining copies of the required documents, LT Hines consults the TNIEG for information regarding the risk assessment procedure that will help him determine the recommended minimum security requirements for VQ-7's LAN. As mentioned earlier, the TNIEG relies heavily on the procedure mandated by DoD Directive 5200.28 Enclosure (4). LT Hines follows the six step risk assessment procedure outlined in the TNIEG.

1. Step 1: Determine system security mode of operation.

Based on the CO's description of desired capabilities for VQ-7's trusted network and the definitions of the different security modes, LT Hines determines that the mode of operation needs to be multilevel. VQ-7's trusted network will need to simultaneously handle multiple levels of classified information (unclassified up through but not greater than secret) in an environment where not all of the users have the clearance, authorization, or formal access approval required. The security mode of operation selected will be verified by step 5.

2. Step 2: Determine minimum user clearance or authorization rating.

Using the Rating Scale for Minimum User Clearance (Rmin) (Table 2, Chapter V), LT Hines determines the Rmin to be 1. VQ-7 is composed of several departments that handle classified documents on a daily basis. However, there

are some departments that provide administrative support to the squadron and do not have a need to handle classified documents. The personnel that provide this administrative support do not have the clearance to handle classified information but do routinely have access to sensitive but unclassified information (e.g., squadron personnel social security numbers and home addresses).

3. Step 3: Determine maximum data sensitivity rating.

The CO stated his desire for a trusted network that would be capable of handling multiple levels of classified information up to, but not greater than secret. Additionally, VQ-7's information sensitivity is considered to be "without categories." LT Hines uses this information to determine VQ-7's Rmax from Table 3 in Chapter V (Rating Scale for Maximum Data Sensitivity (Rmax)). LT Hines finds that Table 3 assigns an Rmax rating of 3 for VQ-7's maximum data sensitivity.

4. Step 4: Determine risk index.

LT Hines now uses the information obtained in steps two and three to determine VQ-7's risk index. Using the formula provided in the TNIEG (Risk Index = Rmax - Rmin), he calculated VQ-7's risk index to be 2 (Rmax (3) - Rmin (1) = 2).

5. Step 5: Determine minimum security evaluation class for computer-based controls.

After LT Hines calculates VQ-7's risk index, he matches this number to the Security Risk Index (Table 4, Chapter V) to verify the appropriate security mode and determine the minimum NCSC-evaluation rating for the system. VQ-7's risk index of 2 matches to a multilevel or partitioned security mode and a minimum security class of B2. Descriptions of the different security modes are provided in Appendix F. Since not all of VQ-7's personnel have clearance,

authorization, or formal access approval for the information to be processed on the LAN, the multilevel security mode is dictated by VQ-7's operational environment.

6. Step 6: Determine adjustments to computer security evaluation class required.

Step six involves a more detailed gathering of information about environmental and architectural risk factors. It includes the analysis of the applications environment and such factors as system allowance for programming and potential restriction to limited sets of applications. This step is considered to be beyond the scope of the ADP officer's assessment of VQ-7's needs at this time and will not be included in further discussions.

E. PHASE I - TNI PART II RISK ASSESSMENT OF VQ-7

1. Functionality

Using the additional security services listed in TNI Part II (and the questions provided in Appendix G), LT Hines determines the functionality required (desired) by the CO. The CO answers these questions with the assistance of LCDR Packard and the Communications Department head. The CO's answers to the Part II questions (Appendix G) identify the desired functionality for each security service. His answers are listed in Appendix I.

2. Strength of Mechanism

Since the risk index calculation for TNI Part II concerns the lowest clearance of non-AIS users that have physical access to any AIS object in the squadron, LT Hines has to consider all squadron personnel, visitors, and the contract personnel that provide support services such as vending and janitorial services. Although security policies require that all personnel without the proper clearances be escorted by squadron personnel who do have clearance, these non-

AIS users still obtain physical access to the squadron AIS. Using the Minimum Clearance for Physical Access table (Table 6, Chapter V), LT Hines determines the R_{min} for Part II to be 0. The minimum clearance for personnel gaining physical access to VQ-7's AIS is Uncleared or Not Authorized.

The Maximum Data Sensitivity table (Table 7, Chapter V), is identical to table 3 used in the TNI Part I assessment of risk. The maximum data sensitivity had not changed and therefore LT Hines determines the R_{max} to be 3 ($R_{max} (3) - R_{min} (0) = 3$).

Using Table 8 in Chapter V, LT Hines determines the Minimum Strength of Mechanism Requirement for a TNI Part II risk index of 3. He matches the risk index of 3 to Table 8 and finds that for all Part II security services selected for VQ-7's computing environment, each service needs to have a "good" strength of mechanism.

3. Assurance

LT Hines determines the minimum assurance requirements for each security service using a similar procedure to the one used in the Part I evaluation above. He matches the TNI Part II risk index of 3 to Table 9 (Chapter V), Minimum Assurance Requirements, to determine the Part II assurance rating. LT Hines notes that a Part II risk index of 3 identifies a need for a "good" assurance.

4. Part II Assurance Rating versus Minimum Part I Evaluation

To complete the risk assessment procedure, LT Hines draws a comparison between the Part I evaluation and Part II assurance rating. Table 10 (Chapter V), Part II Assurance Rating, reveals that the Part II assurance rating of "good" is matched to a minimum Part I evaluation of B2. Since Part I and Part II evaluations calculate R_{min} using different criteria, it would not be surprising to end up with a difference in determined evaluation class (e.g., B1 from Part I vs. B2

from Part II). If a difference had occurred, LT Hines would have determined whether VQ-7's operating environment dictates a Part I or Part II dominance. VQ-7's Part I evaluation and selection of Part II security services, however, resulted in the same NCSC-evaluation class of B2. The additional Part II services requested by the CO do not dictate a different NCSC-evaluation class.

VII. NETWORK RISK ASSESSMENT: ANALYSIS AND CONCLUSIONS

A. OVERVIEW OF FINDINGS

The risk assessment procedure described in the TNIEG provided LT Hines with a structured procedure for evaluating VQ-7's operating environment. It led to the determination that the minimum NCSC-evaluation rating for VQ-7's LAN should be B2. Once the evaluation class (B2) has been determined, the requirements to meet this evaluation class are obtained from the TNI. The overall description of class B2 (Structured Protection) as defined in the TNI [1987] follows:

In class (B2) network systems, the NTCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) network systems to be extended to all subjects and objects in the network system. In addition, covert channels are addressed. The NTCB must be carefully structured into protection-critical and non-protection-critical elements. The NTCB interface is well-defined, and the NTCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration. The following are minimal requirements for system assigned a class (B2) rating.

A detailed description of the minimal requirements for a network system rating of B2 are provided in the TNI. With this information, one of the next tasks for the ADP officer involves a search for commercial computer security products that have been evaluated by the NCSC and satisfy the requirements of both a B2 rating and the specific security services identified in the Part II evaluation. Although the details of this process will not be discussed here, it provides a potential area for future research.

During the review of the computer security guidelines and directives that govern the risk assessment process described in this thesis, an important observation was made. The more recent publications in the Rainbow Series, such as the NCSC -- A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems, identify an increasing requirement for personnel with technical qualifications and experience at the lower levels of the Navy's organization (e.g., aviation squadrons). The proliferation of more complex information technology (e.g., LAN's, trusted networks, and distributed databases) at the aviation squadron level brings with it the need for technically qualified information technology managers and administrators. At this time, there is no evidence that the Navy has recognized this need. The following discussion provides clarity to this observation.

The general structure of the hypothetical squadron, VQ-7, can be considered to be a typical "land-based" Navy squadron. As mentioned earlier, billets in the squadron are typically assigned to officers for a duration that does not usually exceed one year. Although this helps ensure that officers gain a wide variety of experience and helps prevent burnout, it does not provide the squadron with a stable, consistent manager of its Automated Information Systems (AISs) and AIS activities. It can take a newly assigned ADP officer two to three months to become familiar with his/her duties. During this time the squadron will continue to operate without an experienced ADP manager. The training and familiarity that a new ADP officer will receive is provided by the outgoing ADP officer in the form of oral "job turnover" briefings that are conducted over a one to two week period. After this time the new ADP officer is essentially on his/her own. Since there are no formal training courses provided, the ADP officer's success in

providing the squadron with an effective AIS manager is determined solely by his/her personal abilities and motivation to learn the details of the squadron AIS.

Until the recent implementation of the LAN, VQ-7's ADP officer has only had to deal with such tasks as procuring stand-alone desktop computer systems and peripherals, writing and implementing simple squadron computer security policies, and conducting computer security training for squadron personnel. During this time, the squadron has been able to operate effectively while the new ADP officer gained experience. The introduction of newer, more complex computer technology (e.g., LANs, trusted networks), however, may not be conducive to the constant (annual) turnover of ADP officers.

The increasing complexity of the computer technologies being implemented in the Navy's aviation squadrons today (such as LANs) will soon demand ADP personnel with more than just a novice level interest and experience. The person who may be assigned to this type of billet in the near future will receive a new title, Information System Security Officer (ISSO), and will be required to meet certain technical qualifications of both knowledge and experience.

The management of these more complex computer systems will not only require personnel with more technical qualifications, but the length of their assignment to this type of billet will need to be more stable (longer than the typical year). Some important questions come to mind. Where will these technically qualified personnel come from? Will the use of military personnel in these billets provide the needed stability? Will the use of civilians be needed or required?

The people who will fill the ISSO type billets will have previously obtained a computer technology subspecialty. Graduates of the computer technology curricula at NPS Monterey, California are likely military candidates. Military

personnel, however, may have obtained their subspecialty prior to entering the Navy. Technically qualified civilian personnel are also viable candidates for ISSO type billets.

If military officers are specifically assigned to an ISSO billet for a typical three year tour, they will likely provide the necessary stability to the organizations ISSO position. For military officers that have obtained their postgraduate computer technology subspecialty while in the Navy, this type of assignment would essentially be equated to a "payback" tour.

If an increasing demand for technically qualified computer personnel exceeds the existing supply, it may be necessary to rely on the services of civilians in ISSO type billets. This would certainly provide the needed stability for organizations that are implementing more complex computer technology. However, the Navy's budget has been reduced and it may be difficult to acquire specialized civilian personnel when the Navy is mandating cut backs.

As the Navy's aviation squadrons (and other activities) continue to procure and implement new computer technologies, it will certainly be necessary for them to procure qualified personnel to manage them as well. The future requirement to specifically assign officers with computer technology subspecialties to ISSO billets at the lower levels of the Navy's organization may also provide new and more diverse opportunities for postgraduate payback tours.

B. COMMENTS ON THE RISK ASSESSMENT PROCESS

The Technical Guidelines Program is an important effort by the NCSC to channel the research and development of computer security. It has helped to establish clear, common language references and a knowledge base of techniques to be used in the implementation of computer security.

The TNIEG provides a relatively straight-forward method for evaluating the necessary level of trust that must be placed in a LAN. The Part I risk assessment procedure provides a structured way to analyze how an organization's operational environment dictates the minimum requirements for a trusted network. The tables used in steps one through five are well defined and present a clear definition of the minimum security class based on an organizations risk. Step six of the Part I risk assessment procedure, however, is given little discussion. It is intended to provide further refinement to the level of trust required as determined in steps one through five. The NCSC identified the sixth step as a necessary element of the risk assessment procedure, yet it fell short of completing its description in sufficient detail. Instead of providing clarification of this step, the TNIEG simply makes reference to other sources for elaboration. These sources describe a detailed analysis and method to be used in determining the potential need for adjustments to the initial security evaluation class already determined in steps one through five. Without a more detailed discussion and description of step six in the TNIEG, it is unable to provide a self contained source of information and guidance concerning the entire risk assessment procedure. (NCSC, 1990)

The security services outlined in Part II address security concerns that take on increased significance in the network environment. Many of them are outside the scope of Part I or lack theoretical basis and formal analysis underlying the Part I assessment procedure. Although Part II of the risk assessment procedure is discussed in some detail, it still requires further research and development. "... Part II services have not been supported by equally well developed theories and detailed evaluation criteria ..." (NCSC, 1990). As a result the criteria used are very general and somewhat ambiguous. The TNIEG does provide sufficient detail,

however, to identify and enumerate security services that an organization may select for use in its specific environment. The tables used in Part II are also straight forward and provide a relatively simple procedure for conducting the Part II evaluation and for comparing the Part II results to those in the Part I evaluation. Although the TNIEG provides one example of an operating environment that might require a Part II dominance over Part I, it is unclear as to how this dominance is determined in other cases. A more specific guideline or matrix providing correlation between the different security operating modes and Part I verses Part II dominance would be beneficial.

C. DIRECTIONS FOR FUTURE RESEARCH

The plan of attack that LT Hines developed in order to implement a trusted network for VQ-7 involved three phases. Phase I (Determine the NCSC-evaluation rating appropriate for the VQ-7 operational environment) was addressed in this thesis. Detailed discussions of Phase II and Phase III, however, are beyond the scope of this thesis and provide areas for future research efforts.

1. Phase II - Identify, procure, and implement "trusted products"

The sources for identifying trusted computer security products can begin with two of the Rainbow Series publications, NCSC *Trusted Product Evaluation Questionnaire* (NCSC-TG-019) of 1989 and NCSC *Trusted Product Evaluations -- A Guide for Vendors* (NCSC-TG-02) of 1990. In addition, the *Information Systems Security Products and Services Catalogue* and the *Evaluated Products List (EPL)* it contains will provide sources of information.

In 1990, the General Services Administration (GSA) began issuing a series of guides on Federal information resources (IR) acquisitions. The guides are designed to address important aspects of laws, regulations, directives, and policies that establish Federal acquisition requirements. The first of this series, The

Overview Guide, was published in 1990 and provides a description of the acquisition process and the roles and responsibilities of program managers, information resource management, and contracting personnel. This document and others in the series can provide the necessary information for a detailed discussion on information resource acquisition.

2. Phase III - Certification and accreditation (C & A) of trusted systems

DoD Directive 5200.28 directs that a certification plan be designed and implemented in support of the accreditation process. It is to involve a risk analysis of the AIS in its operational environment, an evaluation of the security safeguards, and a certification report. All of these milestones must be approved by the appropriate DAA before classified information may be processed on a trusted network. (DoD, 1988)

DoD Directive 5200.28 also specifies a timetable that shall be adhered to in identifying and implementing required security features. This directive was issued in 1988 and mandated that complete compliance would be required for: (1) existing systems that have already been accredited, within three years from the date of the directive, or (2) new systems, within three years from the date that a system began the design phase of the life-cycle process. (DoD, 1988)

This directive provides for exceptions to its mandated requirements, however. It allows the appropriate DAA to authorize exceptions based on excessive costs of implementation, time constraints of implementation, unsound technical applications of needed security features, or adverse impact on operational effectiveness to an unacceptable degree. The DAA can authorize any or all of these exceptions provided that other safeguards (e.g., physical controls, administrative controls, etc.) can be substituted to attain the required level of system security or protection. (DoD, 1988)

Unfortunately, at the time of its issuance, DoD Directive 5200.28 failed to specify any details concerning the C & A process itself. It simply dictated that activities comply with its contents. The NCSC is only now producing a rough draft technical guideline that introduces C & A concepts in any detail. In short, the Deputy Secretary of Defense issued this directive before the NCSC had developed the procedures and guidance for preparing for, obtaining, and conducting C & A's. The C & A guidance prepared thus far by the NCSC has yet to be formally issued for use. As a result, most activities have obtained waivers from their respective DAA's in order to operate their trusted systems prior to obtaining/achieving certification and accreditation. (Campbell, 1992)

D. FINAL REMARKS

This thesis has described and applied the NCSC's risk assessment methodology to a hypothetical Naval aviation squadron. The results of this assessment identified an NCSC-evaluation class rating appropriate to the squadron's operational environment. The determined NCSC-evaluation class rating (B2) was briefly described and additional NCSC references were cited for elaboration of the specific requirements of this rating.

Other steps, or phases, that might logically follow the NCSC's risk assessment procedure were identified and described briefly. A more detailed discussion of these phases can serve as areas for future research.

An observation concerning the qualifications and experience of personnel assigned to the information technology billets of Naval aviation squadrons identified a factor that may result in potential risk. Personnel that are currently assigned to AIS billets within an aviation squadron do not necessarily meet any specific technical qualification requirements or experience. This situation could make it extremely difficult to effectively and efficiently design, acquire, and

manage newer, more complex information technologies. Additionally, this situation may put the Navy at risk of wasting its resources on unsuitable technologies.

If the Navy continues its course towards implementing more complex information technology at its lower levels, it will need to ensure that the personnel at those levels have the requisite qualifications. The Navy needs to detail qualified personnel to its lower levels ahead of the requirement or desire to design newer, more complex information systems. This will help prevent the design, procurement, and implementation of inadequate information technology (and their security mechanisms) due to a lack of inexperience or knowledge. As mentioned earlier, computer security efforts continue to lag far behind the rapid growth of computer technology in general. Without properly qualified personnel at the squadron level driving information technology and computer security development (at the beginning of its life cycle), implementation, and management, the Navy may be placing itself at a level of IT risk that may be difficult to recover from.

APPENDIX A

RECOMMENDED BACKGROUND READINGS

This thesis does not contain tutorial information on security and networking issues. It is assumed that the reader will have some background in both areas. The references listed below provide background and associated information on security in networks:

Abrams, M.D. and Podell, H.J., Computer and Network Security: a Tutorial, IEEE Computer Society Press, 1987.

Comer, D.E., Internetworking with TCP/IP, Prentice-Hall, 1991.

Davies, D.W. and Price, W.L., Security for Computer Networks, John Wiley & Sons, 1984.

Denning, D.E., Cryptography and Data Security, Addison-Wesley, 1983.

Gasser, M., Building a Secure Computer System, Van Nostrand Reinhold Company, 1988.

Pfleeger, C.P., Security in Computing, Prentice-Hall, 1989.

Russell, Deborah, and Gangemi Sr., G.T., Computer Security Basics, O'Reilly & Associates, Inc., Sebastopol, CA, 1991.

Schatt, S., Understanding Local Area Networks, Second Edition, Howard W. Sams & Company, 1990.

Tanenbaum, S.A., Computer Networks, Second Edition, Prentice-Hall, 1988.

APPENDIX B

NCSC GOALS

The National Computer Security Center (NCSC) was formed to continue the efforts which began with the DoD Computer Security Initiative. The NCSC was chartered by DoD to encourage the widespread availability of trusted computer systems for use by those who process classified or other sensitive information. The NCSC was specifically tasked with the following goals:

- * Encourage the widespread availability of trusted computer systems.
- * Evaluate the technical protection capabilities of industry- and government-developed systems.
- * Provide technical support of government and industry groups engaged in computer security research and development.
- * Develop technical criteria for the evaluation of computer systems.
- * Evaluate commercial systems.
- * Conduct and sponsor research in computer and network security technology.
- * Develop and provide access to verification and analysis tools used to develop and test secure computer systems.
- * Conduct training in areas of computer security.
- * Disseminate computer security information to other branches of the federal government and to industry. (Russell and Gangemi, 1991)

APPENDIX C

OVERVIEW OF COMPUTER SECURITY REGULATIONS, POLICIES AND CRITERIA

A. FEDERAL REGULATIONS

National mandates require the protection of sensitive information, as listed below:

- * Title 18, U.S. Code 1905, makes it unlawful for any office or employee of the U.S. Government to disclose information of an official nature except as provided by law, including data processed by computer systems.
- * Office of Management and Budget (OMB) Circular No. A-130 establishes requirements for Federal agencies to protect sensitive data.
- * Public Law 100-235, The Computer Security Act of 1987, creates a means for establishing minimum acceptable security practices for systems processing sensitive information.
- * Executive Order 12356 prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

B. DEPARTMENT OF DEFENSE SECURITY POLICY

DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs), is the overall computer security policy document for the DoD. The document identifies mandatory and minimum AIS security requirements. Each agency may issue its own supplementary instructions. For DoD agencies, these instructions fall within the scope of the DoD guidelines and add more specificity. Additional requirements may be necessary for selected systems, based on risk assessments.

Additional security documents are:

- * Department of Defense 5220.22-M, Industrial Security Manual for Safeguarding Classified Information.
- * Defense Intelligence Agency Manual (DIAM) 50-4, Security of Compartmented Computer Operations.
- * Director of Central Intelligence Directive (DCID) 1/16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks.
- * The Supplement to DCID 1/16, Security Manual for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks.
- * National Security Agency/Central Security Service (NSA/CSS) Manual 130-1, The NSA/CSS Operational Computer Security Manual.
- * Air Force Regulation (AFR) 205-16, Computer Security Policy.
- * Army Regulation (AR) 380-19, Security: Information Systems Security.
- * Chief of Naval Operations Instruction (OPNAVINST) 5239.1A, Automatic Data Processing Security Program.

C. SECURITY STANDARDS

As previously discussed, the NCSC is responsible for establishing and maintaining technical standards and criteria for the evaluation of trusted computer systems. The Orange Book (TCSEC) defines technical security criteria for evaluating general purpose AISs. The TCSEC became a DoD standard in 1985 and is mandatory for all DoD components. The TCSEC rates computer systems based on an evaluation of their security features and assurances. The TNI interprets the TCSEC for networks and provides guidance for selecting and specifying other security services (e.g., communications integrity, denial of service, and transmission security). (NCSC, 1992)

APPENDIX D

DETAILED DESCRIPTION OF USER CLEARANCES AND DATA SENSITIVITIES

This appendix describes in detail the clearances and data sensitivities (e.g., classification) introduced earlier in this thesis.

A. CLEARANCES

This section defines increasing levels of clearance or authorization of system users. System users include not only those users with direct connections to the system but also those users without direct connections who might receive output or generate input that is not reliably reviewed for classification by a responsible individual.

- * Uncleared (U)--Personnel with no clearance or authorization. Permitted access to any information for which there are no specified controls, such as openly published information.
- * Unclassified Information (N)--Personnel who are authorized access to sensitive unclassified (e.g., For Official Use Only (FOUO)) information, either by an explicit official authorization or by an implicit authorization derived from official assignments or responsibilities.
- * Confidential Clearance (C)--Requires U.S. citizenship and typically some limited records checking. In some cases, a National Agency Check (NAC) is required (e.g., for U.S. citizens employed by colleges or universities).
- * Secret Clearance (S)--Typically requires a NAC, which consists of searching the Federal Bureau of Investigation fingerprint and investigative files and the Defense Central Index of Investigations. In some cases, further investigation is required.
- * Top Secret Clearance based on a current Background Investigation (TS(BI))--Requires an investigation that consists of a NAC, personal contacts, record searches, and written inquiries. A BI typically includes an investigation extending back 5 years, often with a spot check investigation extending back 15 years.

- * Top Secret Clearance based on a current Special Background Investigation (TS(SBI))--Requires an investigation that, in addition to the investigation for a BI, includes additional checks on the subject's immediate family (if foreign born) and spouse and neighborhood investigations to verify each of the subject's former residences in the United States where he resided six months or more. An SBI typically includes an investigation extending back 15 years.
- * One category (1C) - In addition to a TS(SBI) clearance, written authorization for access to one category of information is required. Authorizations are the access rights granted to a user by a responsible individual (e.g., security officer).
- * Multiple categories (MC) - In addition to TS(SBI) clearance, written authorization for access to multiple categories of information is required.

B. DATA SENSITIVITIES

Increasing levels of data sensitivity are defined as follows:

- * Unclassified (U)--Data that is not sensitive or classified: publicly releasable information within a computer system. Note that such data might still require discretionary access controls to protect it from accidental destruction.
- * Not Classified but Sensitive (N)--*Unclassified but sensitive data.* Much of this is FOUO data, which is that unclassified data that is exempt from release under the Freedom of Information Act. This includes data such as the following:
 - Manuals for DoD investigators or auditors.
 - Examinations questions and answers used in determination of the qualification of candidates for employment or promotion.
 - Data that a statute specifically exempts from disclosure, such as Patent Secrecy data.
 - Data containing trade secrets or commercial or financial information.
 - Data containing internal advice or recommendations that reflect the decision-making process of an agency.
 - Data in personnel, medical, or other files that, if disclosed, would result in an invasion of personal privacy.
 - DoD Directive 5400.7 prohibits any material other than that cited in FOI Act exemptions from being considered or marked FOUO. One other form of unclassified sensitive data is that pertaining to unclassified technology with military application. This refers primarily to documents that are controlled under the Scientific and Technical Information Program or acquired under the Defense Technical Data Management Program. In addition to specific requirements for protection of particular forms of unclassified sensitive data there are two general mandates. The first is Title 18, U.S. Code 1905, which makes it unlawful for any office or employee of the U.S. Government to disclose information of an

official nature except as provided by law, including when such information is in the form of data handled by computer systems. Official data is data that is owned by, produced by or for, or is under the control of the DoD. The second is Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum Number 1, which establishes requirements for Federal agencies to protect sensitive data.

- * Confidential (C)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.
- * Secret (S)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.
- * Top Secret (TS)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.
- * One Category (1C)--Applied to Top Secret Special Intelligence information (e.g., Sensitive Compartmented Information (SCI) or operational information (e.g., Single Integrated Operational Plan/Extremely Sensitive Information (SIOP/ESI)) that requires special controls for restrictive handling. Access to such information requires authorization by the office responsible for the particular compartment. Compartments also exist at the C and S levels.
- * Multiple Categories (MC)--Applied to Top Secret Special Intelligence or operational information that requires special controls for restrictive handling. This sensitivity level differs from the 1C level only in that there are multiple compartments involved. The number can vary from two to many, with corresponding increases in the risk involved. (DoD CSC, 1985)

APPENDIX E

TABLE FOOTNOTES

Chapter V

TABLE 3

- 1 Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.
- 2 The only categories of concern are those for which some users are not authorized access. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level. Systems in which all data are in the same category are treated as without categories.
- 3 Unclassified data by definition may not contain categories.
- 4 Examples of N data include financial, proprietary, privacy, and mission-sensitive data. In some situations (e.g., those involving extremely large financial sums or critical mission-sensitive data), a higher rating may be warranted. This table prescribes minimum ratings.
- 5 The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes EXCEPTIONALLY GRAVE damage to U.S. national security, whereas the loss of Secret data causes SERIOUS damage. (NCSC, 1990)

TABLE 4

- 1 Although there is no prescribed minimum class, the integrity and denial of service requirements of many systems warrant at least class C2 protection.
- 2 Automated markings on output must not be relied on to be accurate unless at least class B1 is used.
- 3 Where an AIS handles classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being handled, at least a class B2 is required.

4 The asterisk (*) indicates that computer protection for environments with that risk index is considered to be beyond the state of current computer security technology.

5 Most embedded systems and desk top computers operate in the dedicated mode. (NCSC, 1990)

Chapter VI

TABLE 5

Part II evaluations are qualitative, as compared with the hierarchically-ordered ratings (e.g., C1, C2, ...) from the TCSEC. The results of a Part II evaluation for offered services are generally summarized using the terms "none", "minimum", "fair", and "good". For some services, functionality is summarized using "none" or "present" because gradations are not meaningful. The term "none" is used to mean the security service fails to distinguish the strength of mechanism. The term "not offered" is used when a security service is not offered. For example, if a certain network did not include non-repudiation as one of its security services, that network would be rated "not offered" with respect to non-repudiation.

TABLE 7

1 Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.

2 The only categories of concern are those for which some users are not authorized access. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level. Systems in which all data are in the same category are treated as without categories.

3 Unclassified data by definition may not contain categories.

4 Examples of N data include financial, proprietary, privacy, and mission-sensitive data. In some situations (e.g., those involving extremely large financial sums or critical mission-sensitive data), a higher rating may be warranted. This table prescribes minimum ratings.

5 The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes EXCEPTIONALLY GRAVE damage to U.S. national security, whereas the loss of Secret data causes SERIOUS damage. (NCSC, 1990)

APPENDIX F

SYSTEM SECURITY MODES OF OPERATION

The system security mode of operation for an AIS is determined as follows:

- * Dedicated Security Mode: An AIS is defined as operating in the dedicated security mode if all users have the clearance or authorization, documented formal access approval, if required, and the need-to-know for all information handled by the AIS. The AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. The AIS shall be isolated electrically, logically and physically from all personnel and AISs not possessing the requisite clearance or authorization, formal access approval, if required, and need-to-know for all of the information handled by the AIS.
- * System High Security Mode: An AIS is defined as operating in the system high security mode if all users have the clearance or authorization and documented formal access approval, if required, but not necessarily the need-to-know for all information handled by the AIS.
- * Multilevel Security Mode: An AIS is defined as operating in the multilevel security mode if not all users have the clearance, authorization, or formal access approval, if required, for all information handled by the AIS.
- * Partitioned Security Mode: An AIS is defined as operating in the partitioned security mode if all users possess the clearance, but not necessarily a formal access approval, for all information handled by the AIS. (DoD, 1988)

APPENDIX G

TNI PART II QUESTIONS

This appendix asks questions about each of the security services contained in Part II of the TNI. These questions are designed to help the security manager identify the functionality required for each security service. The questions should be answered in sequence, unless the answer to one question contains an instruction to skip ahead. (NCSC, 1990)

A. AUTHENTICATION

1. Is there a requirement to determine what individual, process or device is at the other end of a network communication? If yes, document this requirement. If no, skip to Communications Field Integrity.
2. Do you have a requirement to identify and authenticate the specific hardware device at the distant end-point involved in the network communication?

If yes, then you have a functionality requirement for authentication. This functionality may be implemented at one or more protocol layer. For example, a specific control character, ENQ (enquiry or who-are-you) may be used to return immediately a stored terminal identifier.

3. Do you have a requirement to identify and authenticate the location of the hardware at the distant end-point or in any intermediate system involved in the network communication?

If yes, then you have a functionality requirement for authentication at protocol layer 2, the Link Layer or layer 3, the Network Layer.

4. Do you have a requirement to identify and authenticate the specific operating system or control program at the distant end-point or in any intermediate system involved in the network communication?

If yes, then you have a functionality requirement for authentication at protocol layer 4, the Transport Layer.

5. Do you have a requirement to identify and authenticate the subject (process/domain pair) at the distant end-point involved in the network communication?

If yes, then you have a functionality requirement for authentication at protocol layer 4 or above.

6. Do you have a requirement to identify and authenticate the application or user at the distant end-point involved in the network communication?

If yes, then you have a functionality requirement for authentication above protocol layer 7, the Applications Layer. The Applications Layer provides an interface to the application. Authentication information may pass over this interface. Authentication of a user is addressed in Part I of the TNI. Application process authentication is outside the scope of the OSI Security Architecture, but does fall within the scope of TNI Part II Security Services.

Have you chosen to use some mechanism other than encryption to provide authentication? If so, your strength of mechanism is shown in Table 8.

If your authentication mechanism is encryption based, see appropriate encryption authority (e.g., NSA). Even if encryption is used, some supporting processes may need to satisfy the strength of mechanism shown in Table 8 (depending on the architecture). For example, a

database that relates encryption keys to specific users may need to be trusted.

B. COMMUNICATIONS FIELD INTEGRITY

1. Do you have a requirement to protect communication against unauthorized modification?

If no, skip to Non-Repudiation.

2. Are your protection requirements the same for all parts of the information communicated?

If no, then you should identify the separate parts and answer the rest of the questions in this section separately for each part. Each part is known as a field.

There are two major fields: protocol-information, wherein the network is informed of the destination of the information and any special services required; and user-data. Not every protocol data unit (PDU) contains user-data, but protocol-information is necessary. Each of these fields may be divided into additional fields; depending on you application, protection requirements for fields may differ.

3. Do you have a requirement for detecting unauthorized modification to part or all of a PDU?

If yes, you have a requirement for at least minimum functionality.

4. Do you have a requirement for detecting any of the following forms of message stream modification: insertion, deletion, or replay?

If yes, you have a requirement for at least fair functionality. In addition, your functionality must be incorporated in a connection oriented protocol.

5. Do you require that, if message stream modification is detected, recovery (correction) should be attempted?

If yes, you have a requirement for good functionality. In addition, you must implement integrity in a reliable transport (layer 4) mechanism.

C. NON-REPUDIATION

1. Do you have a requirement to be able to prove (to a third party) that a specific message transfer actually occurred?

If no, skip to Denial of Service.

2. Do you have a requirement for proving that a specific message was sent? *Specific message* means that the identity of the subject sending the message, the host computer and/or mail agent/server, time and date, and contents are all uniquely and unalterable identified.

If yes, then you have a functionality requirement for non-repudiation with proof of origin.

3. Do you have a requirement for proving that a specific message was received? *Specific message* means that the identity of the subject sending the message, the host computer and/or mail agent/server, time and date, and contents are all uniquely and unalterable identified.

If yes, then you have a functionality requirement for non-repudiation with proof of delivery.

D. DENIAL OF SERVICE

1. Do you have a requirement to assure the availability of communications service or to determine when a Denial of Service (DOS) condition exists? A DOS condition is defined to exist whenever throughput falls below a pre-established threshold, or when access to a remote entity is unavailable, or when resources are not available to users on an equitable basis. For a

DOS condition to occur, the user must have priority to access the system or resources.

If no, skip to Data Confidentiality.

2. Do you have a requirement to detect conditions that would degrade service below a pre-selected minimum and to report such degradation to the network operators?

If yes, you have a requirement for at least minimum denial of service functionality.

3. Could failure of the system to operate for several minutes lead to personal injury or large financial loss?

If yes, you have a requirement for at least fair denial of service functionality.

4. Do you have a requirement for service resiliency that would continue--perhaps in a degraded or prioritized mode--in the event of equipment failure and/or unauthorized actions?

If yes, you have a requirement for at least fair denial of service functionality.

5. Could failure of your system to operate for several minutes lead to loss of life?

If yes, you have a requirement for good denial of service functionality.

6. Do you have a requirement for automatic adaptation upon detection of a denial-of-service condition?

If yes, you have a requirement for good denial of service functionality.

E. PROTOCOL BASED DOS PROTECTION

1. Do you want advanced knowledge of unavailability of service?

If no, skip to Network Management.

If yes, do you want to implement alternatives?

If yes, you should employ this alternative basis and skip to Network Management.

2. In general, ordinary protocol mechanisms don't provide protection against malicious attacks or bizarre errors. Do you have a requirement to detect a DOS condition which cannot be met by the protocols used as part of normal communications?

If no, you do not have a functional requirement for protocol-based DOS protection and should skip to Network Management.

3. The TNI suggests the following protocol-based mechanisms:
 - a. Measure the transmission rate between peer entities under conditions of input queuing, and compare the measured transmission rate with a rate previously identified as the minimum acceptable;
 - b. Employ a request-response polling mechanism, such as "are-you-there" and "here-I-am" messages, to verify that an open path exists between peer entities.

If you have identified any additional mechanisms, include them in your list of required mechanisms.

F. NETWORK MANAGEMENT

1. Do you have a requirement for (at least) detecting a denial of service condition that affects more than a single instance of communication, or attempted communication?

If no, skip to Data Confidentiality.

If yes, you have a functional requirement for network management denial of service protection.

G. DATA CONFIDENTIALITY

1. Do you have a requirement to protect any part of transmitted data from disclosure to unauthorized persons?

If no, skip to Traffic Flow Confidentiality.

2. Is your requirement for confidentiality limited to selected field of user-data within a PDU?

If no, then you require confidentiality for the entire data portion of each PDU. Continue with Traffic Flow Confidentiality.

3. Is there a reason to encrypt only selected fields (e.g., cost savings, legal requirements)?

If yes, you require selected field confidentiality. If no, you require full confidentiality on the data portion of each PDU.

H. TRAFFIC FLOW CONFIDENTIALITY

1. Do you have a requirement to prevent analysis of message length, frequency, and protocol components (such as addresses) to prevent information disclosure through inference (traffic analysis)?

If no, skip to Selective Routing.

If yes, you have functional requirement for traffic flow confidentiality.

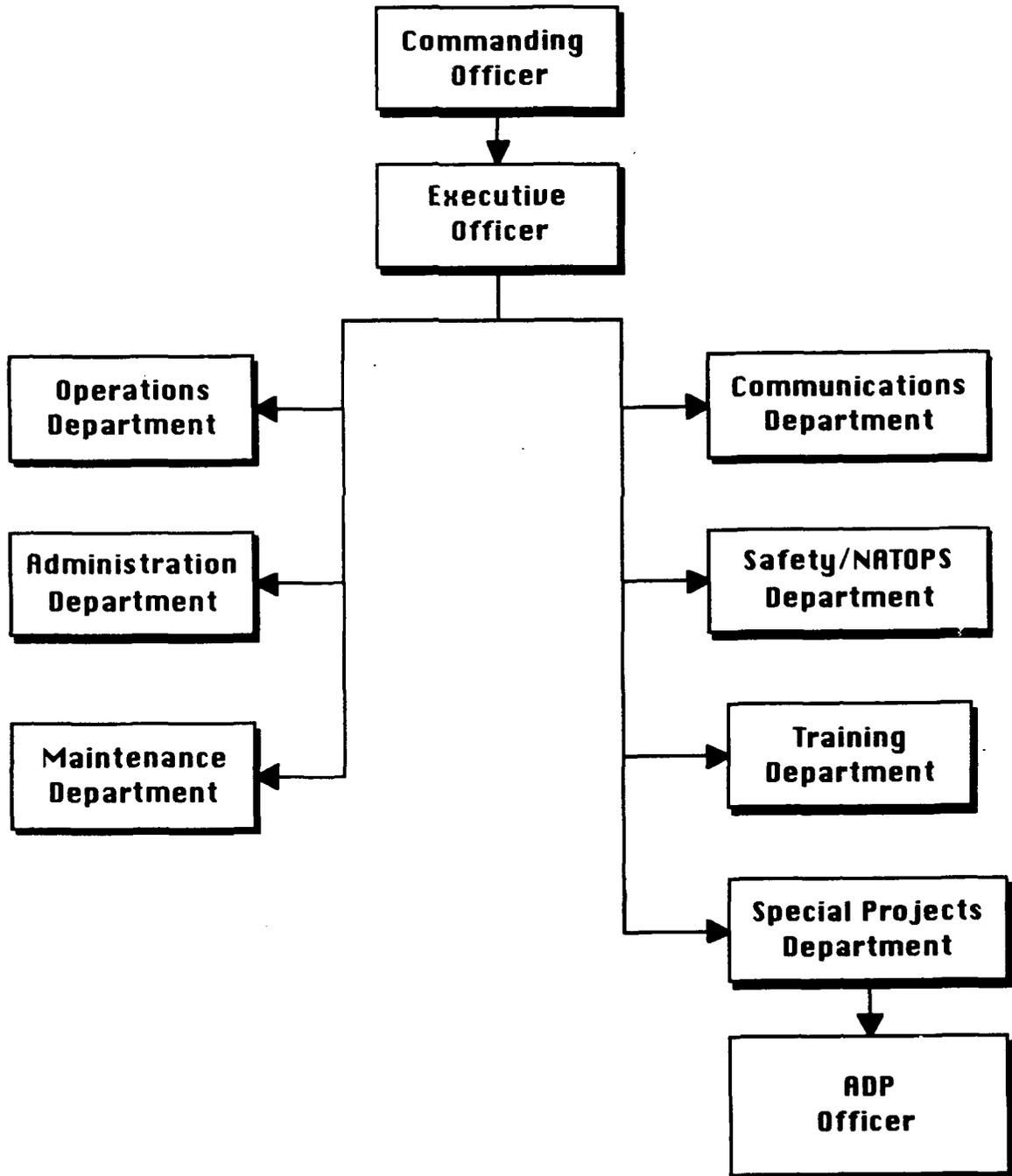
I. SELECTIVE ROUTING

1. Do you have a requirement to choose or avoid specific networks, links, relays, or other devices for any reason at any time?

If yes, you have a functional requirement for selective routing.

APPENDIX H

VQ-7 ORGANIZATIONAL CHART



APPENDIX I

VQ-7 CO ANSWERS TO TNI PART II QUESTIONS

A. AUTHENTICATION

1. Is there a requirement to determine what individual, process or device is at the other end of a network communication? Yes.

2. Do you have a requirement to identify and authenticate the specific hardware device at the distant end-point involved in the network communication?

Yes, VQ-7 has a functional requirement for authentication. This functionality may be implemented at one or more protocol layer. The answers to the following questions will provide this information.

3. Do you have a requirement to identify and authenticate the location of the hardware at the distant end-point or in any intermediate system involved in the network communication?

Yes, VQ-7 has a functional requirement for authentication at protocol layer 2, the Link Layer or layer 3, the Network Layer.

B. COMMUNICATIONS FIELD INTEGRITY

1. Do you have a requirement to protect communication against unauthorized modification? Yes.

2. Are your protection requirements the same for all parts of the information communicated? Yes.

3. Do you have a requirement for detecting unauthorized modification to part or all of a PDU? Yes, VQ-7 has a requirement for at least minimum functionality.

C. NON-REPUDIATION

1. Do you have a requirement to be able to prove (to a third party) that a specific message transfer actually occurred? Yes.
2. Do you have a requirement for proving that a specific message was sent? *Specific message* means that the identity of the subject sending the message, the host computer and/or mail agent/server, time and date, and contents are all uniquely and unalterable identified. Yes, VQ-7 has a functional requirement for non-repudiation with proof of origin.
3. Do you have a requirement for proving that a specific message was received? *Specific message* means that the identity of the subject sending the message, the host computer and/or mail agent/server, time and date, and contents are all uniquely and unalterable identified. Yes, VQ-7 has a functional requirement for non-repudiation with proof of delivery.

D. DENIAL OF SERVICE

1. Do you have a requirement to assure the availability of communications service or to determine when a Denial of Service (DOS) condition exists? A DOS condition is defined to exist whenever throughput falls below a pre-established threshold, or when access to a remote entity is unavailable, or when resources are not available to users on an equitable basis. For a DOS condition to occur, the user must have priority to access the system or resources. Yes.
2. Do you have a requirement to detect conditions that would degrade service below a pre-selected minimum and to report such degradation to the network operators?
Yes, VQ-7 has a requirement for at least minimum denial of service functionality.

3. Could failure of the system to operate for several minutes lead to personal injury or large financial loss? No.
4. Do you have a requirement for service resiliency that would continue--perhaps in a degraded or prioritized mode--in the event of equipment failure and/or unauthorized actions? No.
5. Could failure of your system to operate for several minutes lead to loss of life? No.
6. Do you have a requirement for automatic adaptation upon detection of a denial-of-service condition? No.

E. PROTOCOL BASED DOS PROTECTION

1. Do you want advanced knowledge of unavailability of service?
No, skip to Network Management.

F. NETWORK MANAGEMENT

1. Do you have a requirement for (at least) detecting a denial of service condition that affects more than a single instance of communication, or attempted communication? Yes, VQ-7 has a functional requirement for network management denial of service protection.

G. DATA CONFIDENTIALITY

1. Do you have a requirement to protect any part of transmitted data from disclosure to unauthorized persons? Yes.
2. Is your requirement for confidentiality limited to selected field of user-data within a PDU? Yes.
3. Is there a reason to encrypt only selected fields (e.g., cost savings, legal requirements)? Yes, VQ-7 requires selected field confidentiality.

H. TRAFFIC FLOW CONFIDENTIALITY

1. Do you have a requirement to prevent analysis of message length, frequency, and protocol components (such as addresses) to prevent information disclosure through inference (traffic analysis)? Yes, VQ-7 has a functional requirement for traffic flow confidentiality.

I. SELECTIVE ROUTING

1. Do you have a requirement to choose or avoid specific networks, links, relays, or other devices for any reason at any time?
Yes, VQ-7 has a possible functional requirement for selective routing.

LIST OF REFERENCES

- Arsenault, A. W., *Developments in Guidance for Trusted Computer Networks*, 1987 *Proceedings of the 10th National Computer Security Conference*.
- Campbell, Debbie, CDR USN, Phone Interview, INFOSEC Awareness Division, 1992 *Certification and Accreditation*, National Computer Security Center, Fort Meade MD, August 1992.
- Department of Defense, CSC-STD-004-85 *Technical Rationale Behind CSC-1985 STD-003-85: Computer Security Requirements*. DoD Computer Security Center, Fort Meade MD, June 1985.
- Department of Defense, DOD 5200.28-STD, *Trusted Computer System 1985 Evaluation Criteria*, December 1985.
- Department of Defense, Directive 5200.28, *Security Requirements for 1988 Automative Data Processing (ADP) Systems*, March 1988.
- National Computer Security Center, NCSC-TG-027, Version-1, *A Guide to 1992 Understanding Information System Security Officer Responsibilities for Automated Information Systems* National Computer Security Center, Fort Meade MD, May 1992.
- National Computer Security Center, Technical Report 111-91, *Integrity-oriented 1991 Control Objectives: Proposed Revisions to the Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD*. National Computer Security Center, Fort Meade, MD, October 1991.
- National Computer Security Center, NCSC-TG-011, *Trusted Network 1990 Interpretation Environments Guideline*. National Computer Security Center, Fort Meade, MD, 1 August 1990.
- National Computer Security Center, NCSC-TG-005 *Trusted Network 1987 Interpretation of the Trusted Computer System Evaluation Criteria*. National Computer Security Center, Fort Meade, MD, 31 July 1987.
- National Telecommunications and Information Systems Security (NTISS), 1987 *NTISSAM COMPUSEC/1-87, Advisory Memorandum on Office Automation Security Guideline*. National Security Agency, Fort Mead MD, 16 January, 1987.
- Palmer, I. C., Potter, G. A., *Computer Security Risk Management*, Van Nostrand 1989 Rienhold, New York, NY, 1989.

- Pfleeger, Charles P., *Security in Computing*, Prentice-Hall, Inc., Englewood ,
1989 Cliffs NJ, 1989.
- Russell, Deborah, and Gangemi Sr., G.T., *Computer Security Basics*, O'Reilly &
1991 Associates, Inc., Sebastopol, CA, 1991.
- Seidcon, Inc., *Quick Reference Guide On Developing A Secure System* (Draft
1992 Copy), Huntsville, Alabama, Oceanside, California, 12 June 1992.
- Shannon, Campbell, *An Evaluation of the Need for LAN's at Naval Aviation
1992 Squadrons and Wings*, Master's Thesis, Naval Postgraduate School,
Monterey, California, June 1992.
- Tannis, Daryl C., *An Assessment of the National Computer Security Center's
1988 Approach for Computer Network Security and a Recommended
Alternative Systems Approach*, Master's Thesis, The American
University, Washington, D.C., July 1988.

INITIAL DISTRIBUTION LIST

	No. Copies
1. Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2. Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3. Computer Technology Programs Code 37 Naval Postgraduate School Monterey, California 93943-5002	1
4. Commander Naval Air Force U.S. Pacific Fleet NAS North Island, California 92135	1
5. Department Chairman, Code AS Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
6. Prof. Tung Bui, Code AS/BD Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
3. Prof. William J. Haga, AS/HG Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
4. Prof. Myung W. Suh, AS/SU Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
6. LCDR Mark A. Paylor 2208 W. Mark Rd. Edmond, Oklahoma 73034	4