A Guide to the Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements

Volume 1 of 4

Table of Contents

NCSC-TG-024
Volume 1/4
Library No. 5-239,669
Version 1

FOREWORD

This guideline, volume 1 of 4 in the series, "A Guide to Procurement of Trusted Systems," is written to help facilitate the acquisition of trusted computer systems in accordance with DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria." It is designed for new or experienced automated information system developers, purchasers, or program managers who must identify and satisfy requirements associated with security-relevant acquisitions. Information contained within this series will facilitate subsequent development of procurement guidance for the Federal Criteria. This series also includes information being developed for certification and accreditation guidance. Finally, this introductory guideline addresses both the complex acquisition process and the many regulations, standards, and criteria to be satisfied in providing a secure system.

There is a large body of national policy established in the form of regulations, directives, Presidential Executive Orders, and Office of Management and Budget (OMB) Circulars that forms the basis for procedures to handle and process Federal information, particularly classified information. These are presented and discussed in Appendix A, "Historical Basis."

The business of computers, security, and acquisitions is complex and dynamic. As the Director, National Computer Security Center, l invite your recommendations for revision to this technical guideline. Our staff will work to keep it current. However, experience of users in the field is the most important source of timely information. Please send comments and suggestions to;

National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6000
ATTN: Standards, Criteria, and Guidelines Division

December 1992

Patrick R. Gallagher
Director
National computer Security Center

ACKNOWLEDGEMENTS

This document has been produced under the guidance of Major (USA) Melvin L. DeVilbiss, assisted by CPT (USA) Michael Gold and Mary Whittaker, from the National Security Agency. Much of this document is taken directly from "Computer Security in Acquisitions (Draft)," prepared by the Air Force Intelligence Command (AFIC), Air Force Cryptologic Support Center, Directorate of Securities (AFCSC/SR), under the direction of Captain (USAF) Bob Pierce. Initial ideas for the Air Force draft document were those of TRACOR, Inc. Interpretation and adaptation as a DoD handbook was accomplished by Howard Johnson, Information Intelligence Sciences, Inc.

The following organizations were particularly helpful in providing constructive reviews and advice: Harris, Grumman Data Systems, CTA, Inc., Seidcon, Naval Computer and Telecommunications Command, Naval Electronic Systems Security Engineering Center, U.S. Army Information Systems Engineering Command, GSA, MlTRE, Federal Emergency Management Agency, and Logicon.

Special thanks to Carol Oakes, Senior Technical Editor, MITRE, for her assistance with final editing of this guideline.

LIST OF FIGURES

LIST OF TABLES

1 GENERAL INFORMATION

1.1 INTRODUCTION

This document is a guideline designed for those who must identify and satisfy deliverable data requirements associated with security-relevant acquisitions of trusted, stand-alone systems. It identifies what must be complied with, what must be read, what must be written, and what others must be instructed to write. The detailed acquisition process, coupled with the technical complexity of computers, security, and contracting, represents an unsolvable mystery for many. The goal of this document is to help clarify the complex issues.

The National Security Agency (NSA) wants to clarify the computer security aspects of the Department of Defense (DoD) Automated Information System (AIS) acquisition process. Therefore, it is producing the guideline series (shown in Table 1-1), of which this document is the first.

Table 1-1 Procurement Guideline Series

An Introduction to Procurement Initiators on Computer Security Requirements (December 1992)
Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators (To be published in 1993)
Computer Security Contract Data Requirements List and Data Item Description Tutorial (To be published in 1993)
Row to Evaluate a Bidder's Proposal Document - An Aid to Procurement Initiators and Contractors (To be published in 1993

1.2 DEFINITION OF TERMS

National Computer Security Center (NCSC)-TG-004, "Glossary of Computer Security Terms," defines security terms used in this publication. DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," defines acquisition terms. DoD Instruction 5000.33, "Uniform Budget/Cost Terms and Definitions," defines budget terms.

1.3 APPLICABILITY

This guideline is for use by all DoD agencies. It applies to AlS developers purchasers, or program managers who deliver systems to customers. It specifically supports acquisitions of systems from commercial-off-the-shelf (COTS) products on the Evaluated Products List (EPL).

1.4 PURPOSE

Figure 1-1 shows how to use this document. The purpose of this document is to provide the Program Manager and the Security Manager a guide to the activities and the documentation in an acquisition of a secure system. This document will help those responsible to develop plans and procedures for acquisition of trusted, stand-alone systems. Specifically, it will help identify security-relevant data to be delivered by a contractor.

Chapter Titles	Who They Should Help
General Information	Introduction to Acquisition
The Acquisition Process	(e.g., for security specialist)
Computer Security	
Threat Risk Mgmt.	Introduction to Security
Security Test & Eval.	(e.g., for acquisition specialist)
Certification &	
Accreditation	
	Guidance for Acquisition
Managing the Acquisition of	of a Secure System
Secure Systems	(e.g., for program and security
	managers)

Figure 1-1 How to Use This Guideline

The second in this series of documents provides a way to specify security requirements accurately in a standardized way, while complying with current acquisition regulations. The Government decides the split of responsibility between the Government and the Contractor. Once documents the contractor is required to write have been identified, a Data Item Description (DID) can be chosen from the third document in this series. If a document is not available, the third document will also help tailor an existing DID to create the desired DID. The fourth document in this series provides a guide to evaluate contractor proposals addressing computer security (COMPUSEC). The fourth guideline is intended for the procurement initiator, but will also be helpful to the contractor preparing his/her proposal.

1.4.1 ASSUMPTIONS

Most users will be building a Request for Proposal (RFP) and therefore will need to develop deliverable data packages. The security functional requirements must have been previously established.

1.4.2 ACQUISITION MANAGEMENT OFFICE

The people reading this document will most likely be assigned to a Program Management Office (PMO) or System Program Office (SPO). These organizational elements are responsible for managing acquisition activities. The PMO/SPO could be a several hundred person organization, or it could be just one person. In either case, the principles and concepts are basically the same; only the scale might change.

1.5 SCOPE

This set of four acquisition documents does not address the complex acquisition of multiple security entity systems. The reason is that the DoD policy has not been finalized that addresses systems with combinations of EPL products and "built and certified" system entities, perhaps using different division/class criteria as requirements from DoD 5200.28-STD. Strong motivation exists to resolve the problem with an NSA-evaluated product on the EPL. Because this resolution cannot be guaranteed, these acquisition documents must deal with a single-system entity (called "the product" or "the system"). In this context, little difference exists between the terms "computer system" and "automated information system," both used here. Section 3.8, "Rationale for Single Entity Approach," presents the rationale for this approach. Chapter 5 addresses use of the EPL.

1.6 REGULATORY HIERARCHY

Regulations may be written for a major system acquisition, an AlS, a computer system, or only the software in a computer system. These entities must be thought of as a nested hierarchy. If the scope is a computer system, for example, then AS and major system regulations also apply. A similar situation exists in security. Regulations deal with information system security (INFOSEC), AlS security, and COMPUSEC. These entities are nested when applied to applications. Considering the system hierarchy and the security hierarchy, a situation exists that is illustrated in Figure 1-2. Thus, requirements for a COMPUSEC acquisition must consider, for example, DoD Instruction 5000.2, DoD 5200.1-R, DoD Directive 5200.28, Figure 1-2 Layers of Regulation DoD-STD-21 67A, and DoD 5200.28-STD.

1.7 OVERVIEW OF THE GUIDELINE

This guideline has seven chapters, and three appendices. Each chapter contains pertinent references. The text focuses on the chapter's subject, incorporating both acquisition and security. Note that Chapter 2 primarily addresses the acquisition process, although it is sometimes placed in the context of security. Chapters 3 through 6 emphasize security, especially in Chapter 3, which addresses security functionality. The two topics finally merge in Chapter 7. Table 1-2 identifies chapters and objectives.

Table 1-2 Guideline Overview

Chapter l General Information - Introduces the guideline.

Chapter 2 The Acquisition Process - Provides an overview of the acquisition process. Identifies the major elements of financial management. It also briefly describes the most important documents to be referenced, produced, or requested when working on a security-related acquisition.

Chapter 3 Computer Security - Provides insight to trusted computing bases (TCBs) and other trusted protection. Discusses the various TCB divisions/ classes and security policy.

Chapter 4 Threat Risk Management – Analysis, Design, and Implementation – Discusses the key aspects of risk management. Addresses the areas of sensitivity levels, risk assessment, risk analysis, and cost benefit analysis.

Chapter 5 Security Test and Evaluation – Addresses the full range of ST&E, single product evaluation, project inception, and system implementation. Also presents a simplified approach to generating contractor test plans.

Chapter 6 Certification and Accreditation – Covers the certification and accreditation processes. It also provides a useful list of documents required for a complete certification or accreditation package.

Chapter 7 Managing the Acquisition of Secure Systems – Discusses the management policy and objectives. Identifies how to prepare plans and concepts. Provides an overview of all security activities associated with the life-cycle process.

1.8 HOW TO GET HELP

This document will not answer all the questions or solve all of the problems encountered in an acquisition. Other sources follow.

1.8.1 REFERENCE SOURCES

Each chapter lists the most important references for the chapter's subject matter. Having a personal, current copy of many of the references is important. The documents will be referred to often. The "must have" list, referenced below in the last section of this chapter, is a good place to start.

1.8.2 MAJOR AGENCY OR ORGANIZATION COUNTERPARTS

Every major agency or organization has several offices that can be of assistance:

a. Each organization usually has a security focal point. Some offices specialize in most aspects of COMPUSEC. Start with a phone call to the Director's office and ask for a directory or a list of offices with names and phone numbers.

b. The investigative organization (e.g., security police) sometimes has experts in applicable areas.

c. Each organization normally has a contracting staff and a planning and budget management staff with expertise in the acquisition process.

d. The user should have a point of contact for the system or project.

1.8.3 SENSITIVE COMPARTMENTED INFORMATION (SCI)

When SCI information is involved, consult the supporting Special Security Officer (SSO) or Intelligence Staff Officer (ISO) within the organization with whom the responsibility has been delegated.

1.8.3.1 SCI REQUIREMENTS

The SSO can assist with the special clearances, handling, storage, marking, and other details required for SCI. The SSO should know how to meet Director of Central Intelligence (DCID) 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," and Defense Intelligence Agency (DIAM) 50-4 "Security of Compartmented Computer Operations."

1.8.3.2 THREAT SUMMARY

The SS0 will be able to assist in requesting an "intelligence community" threat summary related to an individual project. See Chapter 4, "Threat Risk Management," for more on this subject.

1.8.4 OTHER PROGRAM OFFICES

Other PMOs or SPOs are lucrative information sources. Contact the program offices for information on how they have handled similar requirements

1.8.5 NSA

If additional help is still needed, call or write NSA (at the address shown in the Foreword page of this guideline). This organization can usually put you in contact with the right person and get you back on track.

1.9 REQUIRED DOCUMENTS

Very few PMOs or SPOs have a complete suite of reference material. There are, however, a few "must have" documents for all program offices. This document listing will help those new to acquisition, who are working on computer security in an acquisition environment. Appendix A contains a more complete list of historical documents. Working and agency/protection-specific bibliographies are provided in Appendix C at the end of this document.

a. DoD 5200.1-R, "Information Security Program Regulation" - This document is the basic DoD information security regulation, authorized by DoD Directive 5200.1.

b. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)" - This document is the overall security policy document for DoD AlSs that process Classified, sensitive unclassified, or unclassified information, with the exception of certain standalone and embedded computers.

c. DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria" - This document categorizes AISs into hierarchical classes based on evaluation of their security features and assurance for believing the security functionality has been achieved. It is often used to help state the security requirements for any ASs to guarantee satisfaction of a certain minimum risk level.

d. NCSC-TG-005, "Trusted Network Interpretation of the Trusted Computer System

Evaluation Criteria" - This document, also called the "TNI," interprets the DoD 5200.28-STD for networks.

e. NCSC-TG-009, "Computer Security Subsystem Interpretation" - This interpretation of DoD 5200.28-STD is used when a subsystem is to be added to a protected AIS to enhance its security. This document is useful in identifying subsystem security requirements.

f. NCSC-TG-024, Version-1 Vol. 1/4, "A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements," (this guideline) Vol. 2/4, "A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement lnitiators," (draft)

Vol. 3/4, "A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial," (draft)

Vol. 4/4, "A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document - An Aid to Procurement lnitiators and Contractors," (draft)

g. DoD Directive 7920.1, "Life Cycle Management of Automated Information Systems (AIS)" - This document defines life-cycle phases and policy for AISs.

h. DOD Directive 5000.1, "Defense Acquisition" - This directive provides policy and an overview for integrating the efforts and products of 1) requirements generation, 2) acquisition management, and 3) planning, programming, and budgeting systems.

i. DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures" - This instruction implements the regulations of DoD Directive 5000.1 and contains DoD acquisition management policies and procedures, replacing many past regulatory documents.

j. DoD Manual 5000.2-M, "Defense Acquisition Management Documentation and Reports" - This manual contains procedures and formats to be used to prepare various milestone documents and periodic status reports.

k. DoD-STD-2167A, "Defense System Software Development" - This software development regulation establishes requirements to be applied during acquisition, development or support of software standards.

i. DoD 7935-A STD, "ADS Documentation Standard" - This standard provides guidelines for the development and revision of documents for an automated information system.

m. "Model Framework for Management Control Over Automated Information Systems," President's Council on Management Improvement and the President's Council on Integrity and Efficiency, 1988 - This report identifies 55 requirements Federal managers should follow. This list is derived from the Financial Integrity Act of 1982, the Privacy Act of 1974, OMB Circulars A-I 23, A-I 27, and A-I 30.

n. "Information Systems Security Products and Services Catalogue," prepared by the National Security Agency - Complete editions are printed in January and July. Changed chapters from the basic document are reprinted as a supplement in April and October. A large part of Chapter 4, in this catalogue, contains the Evaluated Products List for Trusted Computer Systems. Many trusted system requirements can be effectively met, using existing evaluated products from this source document.

o. "Federal Acquisition Regulation" (FAR) and "DoD FAR Supplement."

p. Federal Information Processing Standard (FIPS) Publication (PUB) 73, "Guidelines for Security of Computer Applications," United States (U.S.) Department of Commerce, National Bureau (NBS) - Planning, development and operations of Federal computing applications requires protection because of the nature of the data or the risk and magnitude of loss or harm. This document addresses risk analysis, objective and vulnerability specifications, management of programming trusted computing systems, and contingency planning.

q. "Federal Information Resources Management Regulation," (FIRMR) General Services Administration (41 CFR 201).

2 THE ACQUISITION PROCESS

2.1 INTRODUCTION

DoD acquisitions are worth billions of dollars each year. Nearly 98 percent of these acquisitions are small contracting efforts worth less than $25,000. That accounts for only 20 percent of DoD's procurement dollars. The other two percent of DoD's contract actions (those over $25,000) account for 80 percent of the dollars. The large dollar contracts bring with them a large number of people and requirements that the program manager must deal with efficiently and effectively. This chapter provides a brief overview of the acquisition process and the environment one can expect to encounter. It provides information on financial management concepts. It also introduces the major documents to be prepared during acquisition.

2.2 ACQUISITION PARTICIPANTS

DoD Directive 5000.1, Part 2, discusses three separate decision making support systems: Planning, Programming and Budgeting (PPBS); Requirements Generation; and Acquisition Management. (See Figure 2-1, taken from that directive.)

Requirements Generation System	Very Broad Needs	Performance Objectives	Requirements	
	Studies	Prototyping	Design & Test	P
				R
Acquisition Management	Alternative Concepts	Concept Selection	Stable Design	O D

System U

Resource Requirements & Constraints C

T

I

Programming & Budgeting System | Affordability Goals | Affordability Constraints | Firm Unit Costs | O N

Figure 2-1 Key Interactions

2.2.1 PLANNING, PROGRAMMING AND BUDGETING

PPBS is supported by three operational functions: 1) the Action Officer (AO) is the primary advocate of a particular program. He/she develops a Program Decision Package (PDP) and presents it to senior management. 2) The Program Element Monitor (PEM) is the functional staff advocate. The PEM guides and monitors PDPs through the PPBS process. When a PDP is approved, the PEM monitors and briefs its progress (e.g., quarterly). The AO needs to stay in contact with the PEM to ensure the latest information is available. 3) The Resource Advisor (RA) is the person in the SPO or PMO who monitors the use of resources on a day-to-day basis, helps develop fund targets, and prepares the annual budget submission.

2.2.2 REQUIREMENTS GENERATION

The mission users are present in all acquisitions. They generate mission requirements and ultimately receive and use the item or services acquired. The user function may be represented by a functional area expert, a major organization (e.g., agency), or even a special office. The user sometimes maintains a liaison in the Program Office.

2.2.3 ACQUISITION MANAGEMENT

This function can be further divided into Program Management and Contract Management. 1) The program management function could have any of several names - PMO, SPO, or Program Office. In a large acquisition, the program management function is a separate organization staffed with specialists who are tasked to conduct the acquisition. In a small acquisition, it could be one person. 2) A contracting function is present in all acquisitions and usually includes a Contracting Officer and a Buyer. The contracting function may be located within the program management organization or within a special contracting activity. The Contracting Officer is the ~ person authorized to obligate the Government (i.e., negotiate, modify, and sign contracts). It is important to seek the Contracting Officer's advice and assistance early to avoid later problems.

2.3 FINANCIAL MANAGEMENT

A structured process of identifying financial requirements, obtaining funds, and allocating them to competing programs (so top priorities are satisfied) is called the PPBS. The PPBS is the official DOD resource management system and is described in DoD Instructions 7045-7 and 7045-14. The PPBS is a complex and continuous year-round process. It involves people from the President all the way down to individual organizations. The PPBS operates in both a top-down and a bottom-up mode. 1) In the top-down mode, high level DoD officials prepare policy and strategy documents. Those documents consider the threats to the worldwide national interests and define the strategy and objectives necessary to counter those threats. 2) In the bottom-up mode, a particular organization tracks every penny it spends. "Fund cites," noted on every document, involves a financial transaction (e.g., travel orders and contracts). The process is complicated, but it achieves visibility and accountability for every expense. The information collected is required by law to be rolled into successively broader accounting Categories and used for tracking appropriations, both for historical purposes and for planning future programs.

2.4 CONTRACTOR/GOVERNMENT INTERFACE

All acquisitions involve dealing with the information processing industry, known as Offerors or Contractors. Their organizations have similarities to Government organizations. They will generally have contracting, program management, and functional (technical) personnel. However, a business relationship with them is not the same as a working relationship with another Government office.

2.4.1 BEFORE CONTRACT AWARD

Civilian corporations can track potential Government contracts using the following sources.

2.4.1.1 MAILING OR BIDDER'S LISTS

Corporations can get on a mailing list at any Government contracting office. The contracting office then sends the corporation solicitations for the types of items or Services the corporation provides.

2.4.1.2 COMMERCE BUSINESS DAILY

The Commerce Department publishes a newspaper called the "Commerce Business Daily" (CBD). The CBD is available to civilian organizations by subscription. Every open acquisition with an estimated value over $25,000 must be advertised in that paper. The CBD also lists potential subcontracting opportunities with major defense contractors. The Program Manager normally prepares a synopsis for the Contracting Office to submit for publication.

2.4.1.3 SMALL BUSINESSES

Smaller corporations can participate in large procurements as subcontractors. Local contracting offices, the Commerce Business Daily, and the Small Business Administration provide leads and contacts that small corporations can pursue.

2.4.2 DURING SOURCE SELECTION

During source selection, the interface with the Offerors is strictly controlled and limited to the Contracting Officer or his/her designee. Some formal communications between the Government and the Offeror(s), usually relate to clarifying the Offeror's proposal. Often a Government central point of contact for technical matters is identified, known as the Contracting Officer's Technical Representative (COTR). However, the COTR does not have the authority to obligate the Government.

2.4.3 AT CONTRACT AWARD

Two important meetings are conducted at contract award.

2.4.3.1 POST-AWARD DEBRIEFING

Security technology is often an eliminator in competition. This session provides feedback for industry on how well, in general terms, their responses met the Government's requirements. The Program Manager should attend the debriefing and be prepared to provide "lessons learned" from the security vantage point. This process will help the industry representatives understand where they were responsive and where improvements can be made. The purpose is not to recite all the details, but to point out security strengths and weaknesses noted in the evaluation of Offerors' proposals.

2.4.3.2 AWARD CONFERENCE

This meeting is the first formal exchange between the Government and the successful Offeror, which is now termed the "Contractor." The Program Manager should attend the meeting to ensure that security issues are addressed and reflected in the minutes.

2.4.4 AFTER CONTRACT AWARD

After contract award, interface with the Contractor is somewhat easier. Keep the following issues in mind.

2.4.4.1 OBLIGATING THE GOVERNMENT

No one may obligate the Government except a Contracting Officer.

2.4.4.2 CONTRACT SCOPE

Specification of security is extremely difficult. What has been given to the contractor in an RFP, or the response, may later prove to be inadequate. The implications of a modification may be great, increasing significantly the effort the contractor originally proposed. The result is another negotiation -- bargaining with security and dollars as the chips. Diluting security is not an option. Neither is overinflated security costs. From the Government's standpoint, two solutions apply: adequate specification in the first place or, if that has not happened, technically astute trade-offs and cost effective technological innovation. This is the most important time to call on security expertise.

2.4.4.3 TECHNICAL INTERCHANGE MEETING

The safest way to communicate with a Contractor is via a Technical Interchange Meeting (TIM). A TIM is formal and requires preparation of minutes that document the proceedings. The Contractor usually prepares these minutes and the Contracting Officer reviews the minutes to ensure that changes in contract scope have not been made.

2.4.4.4 CONTRACT CHANGES

The Government initiates most contract changes. Exceptions include Contractor-proposed engineering changes. Changes may be necessary to clarify, correct, or change requirements or schedules. All changes require the same care and review as the original RFP.

2.4.4.5 INFORMAL CONTACT

Telephone calls, face-to-face meetings, and general correspondence are frequently used for informal discussions of technical and administrative matters. Both parties must be careful not to exceed the limits of their authority. If a question arises about what may be discussed, consult the Contracting Officer in advance.

2.5 DOCUMENT PREPARATION

A large number of documents must be prepared for most acquisitions. Most can be scaled up or down according to the size, scope, and particular needs of individual programs. Appendix B provides an overview of the most important and widely used documents for each of the four major areas, respectively: planning and financial management, program management, mission user, and contracting. Appendix B includes major references to help document preparation. Subsequent paragraphs discuss the documents most important to the user of this guideline. These key documents are usually required for "most" programs. Smaller programs could either combine or reduce the size of individual documents according to the needs of the program.

2.5.1 PLANNING AND FINANCIAL MANAGEMENT DOCUMENTS

These documents provide guidance to people in the organization responsible for conducting acquisition activities.

2.5.1.1 POLICY AND STRATEGY DOCUMENTS

In the top-down mode, high-level DoD officials prepare policy and strategy documents, which include National Security Decision Directives, Defense Guidance, and the long-term (e.g., five year) Defense Program. They consider the threats to worldwide national interests, and define the strategy and objectives necessary to counter those threats.

2.5.1.2 THE PROGRAM OBJECTIVE MEMORANDUM (POM)

The POM provides the response, listed in priority order, to the DoD planning documents.

2.5.1.3 PROGRAM DECISION MEMORANDUM

The DoD then adjusts the POM to ensure each organization's plans are consistent with DoD guidance. The results are published as the Program Decision Memorandum.

2.5.1.4 BUDGETS

Budget estimate submission and final publication of the Budget are the next steps in the process.

2.5.1.5 APPROPRIATIONS

Appropriations are legal authority from Congress to spend dollars on specific line items, or for specific programs. Appropriations to an organization are the result of the budget submission, often followed by a long negotiation process. An appropriation category helps define how funds will be spent. Congress enacts Public Laws to appropriate funds formally to specify these categories.

2.5.1.6 OBLIGATION AUTHORITIES

The DoD passes funds via documents called "Obligation Authorities (OAs)." At the lowest organizational level, the target dollars an organization has available to spend are usually distributed quarterly.

2.5.1.7 PROGRAM DECISION PACKAGE

The PDP, used in conjunction with budget submissions, explains what is needed, why it is needed, and the impact to the functional area operational mission if the program does not receive funding. The PDP is the basic input to the PPBS. Although the Organization responsible for planning and financial management (e.g., Plans) writes the PDP, Program Management input is normally solicited. The document should be kept current. The dollar figures in the PDP must be supportable and the words must be as compelling as the need.

2.5.2 PROGRAM MANAGEMENT DOCUMENTS

These documents provide guidance to the people in the organization responsible for conducting acquisition activities.

2.5.2.1 PROGRAM MANAGEMENT DIRECTIVE (PMD)

The PMD is the first document that authorizes a program to begin. The Program Manager should get a copy and review it thoroughly to determine the program participants and their roles, the basic operational objectives, schedule and milestones, and the resources (both people and dollars) approved by the acquiring organization. The PMD usually identifies a series of supporting plans to be written (e.g., the Test and Evaluation Master Plan (TEMP)). If security is a major concern, a separate section of the PMD will address this topic.

2.5.2.2 PROGRAM MANAGEMENT PLAN (PMP)

The PMP is written in response to tasking cited in the PMD. The PMP amplifies the roles, responsibilities, tasks, and objectives called out in the

PMD. The PMP specifically describes the organizations, players, and assigned tasks. Like the PMD, the PMP often lists a number of supporting plans, identifies who will prepare them, and gives dates for submission (e.g., Human Systems Integration Plan, Program Protection Plan, Software Development Plan, Systems Engineering Management Plan, Technology Assessment and Control Plan, Training and Development Plan, and Risk Management Plans). Security-relevant issues are often described in broad terms. Based on this general guidance, the Program Manager will prepare security- relevant chapters or annexes for a number of support plans.

2.5.2.3 CONFIGURATION MANAGEMENT PLAN (CMP)

The CMP provides both high-level and detailed procedures for developing the baseline the system and identifying, processing, and controlling system changes. Usually, the CMP will identify a Configuration Control Board (CCB), which is responsible for the administrative processes, and serves as a technical body to evaluate proposed changes. As the security focal point, the Program Manager should serve as a member of the CCB to ensure that security-relevant issues are adequately addressed. He/she may also be asked to evaluate changes to assess their "security impact."

2.5.2.4 SOURCE SELECTION PLAN (SSP)

The SSP describes the Source Selection Organization, its roles, functions, responsibilities, and the overall strategy for evaluating proposals (the topic of volume 4 of this guideline series). Normally, the 55P calls for several teams of people to participate in the Source Selection Evaluation Board (SSEB). Typically, these teams will be functionally organized, for example, responsible for technical, management, and cost issues. The SSP also outlines award criteria and evaluation factors along with a scoring methodology. The Program Manager should prepare input for the security-relevant portions of the SSP. The Program Manager may also chair the Security Panel of the Technical Team.

2.5.2.5 PROPOSAL EVALUATION GUIDE (PEG)

Derived from the SSP, the PEG contains detailed procedures on the SSEB's operation. The PEG describes the composition of the evaluation teams, their subordinate panels, and their operating rules. The PEG contains the specific evaluation standards and factors against which Offeror proposals will be judged. The Program Manager should prepare and coordinate the evaluation standards for security matters. Typically, these standards would be used predominately in the Technical Area. However, several Management Area standards must be prepared as well (e.g., an Offeror must describe his/her compliance with DoD 5220.22-M, the Industrial Security Manual). Above all, the Program Manager's role in providing (or coordinating for) evaluation criteria and standards must not be neglected. After contract award, it will be too late to correct discrepancies or oversights without the Contractor justifiably seeking "fair and equitable" compensation for errors. Furthermore, it must be ensured that an Offeror is selected whose proposal best meets the Government's requirements. The PEG is the vehicle to ensure that outcome.

2.5.2.6 ACQUISITION DECISION MEMORANDUM

This memorandum represents approval of a particular milestone phase and authorization for a program to move into the next milestone phase.

2.5.2.7 ACQUISITION PROGRAM BASELINES

Baselines embody the cost, schedule, and performance objectives for a program and should be approved by the milestone decision authority at milestone reviews. Baselines include the Concept Baseline, the Development Baseline, and the Production Baseline.

2.5.2.8 COMPUTER RESOURCES LIFE-CYCLE MANAGEMENT PLAN (CRLCMP)

Like the PMD, the CRLCMP focuses on managing computer resources used in systems throughout their individual life cycles. That is, the CRLCMP identifies the resources, responsible supporting organizations, and the overall strategy to ensure adequate life-cycle support is available. Also, similar to the PMD, the CRLCMP has a subordinate document that provides detailed support procedures. This document, called the Computer Resources Integrated Support Document (CRISD), describes in detail the organizational tasks and procedures for life-cycle support of the computer resource.

2.5.2.9 TEST AND EVALUATION MASTER PLAN (TEMP)

As prescribed by the PMD, the TEMP is the principal source of information for all testing activities. The TEMP describes the complete suite of tests, the test objectives, and cites the organizations that will participate in the testing program. Depending on the testing program scope, the TEMP may have a separate chapter or annex that describes security testing. The Program Manager should beCome familiar with the TEMP and be prepared to provide test plans, test data, and test procedures for the security-relevant concerns and issues identified in the TEMP.

2.5.2.10 INTEGRATED LOGISTICS SUPPORT PLAN (ILSP)

The ILSP addresses reliability, maintainability, and sustainability for the AIS. The plan also describes the maintenance, supply, transportation, training, packaging, and other support capabilities required to Operate and maintain the secure AIS. The Program Manager should ensure security-relevant issues are addressed in the ILSP (e.g., methods for shipping classified devices to a depot for repair).

2.5.3 MISSION USER DOCUMENTS

These documents describe the required Capabilities, functions, and features of the secure AIS. Both DoD Instruction 5000.2 and DoD-STD-7935A will be helpful in preparing these documents.

2.5.3.1 MISSION NEED STATEMENT (MNS)

This non-system specific statement establishes a new operational capability or improves an existing capability.

2.5.3.2 JUSTIFICATION FOR MAJOR SYSTEMS NEW START

This documentation describes a full range of alternatives before deciding to initiate a new acquisition. The justification describes operational needs, projected threats, and plans to identify and research alternative concepts for POM submission. This is supported by the "Federal Information Resources Management Regulation," (FIRMR) (Code of Federal Regulations (CFR) 201, Chapter 29) requirement to conduct a Requirement Analysis and an Analysis of Alternatives.

2.5.3.3 SYSTEM THREAT ASSESSMENT REPORT (STAR)

A threat assessment is required for all major programs. Historically, the STAR has not placed adequate emphasis on COMPUSEC. Identifying the threat of malicious logic attacks (e.g., viruses, worms, and Computer misuse) is important to the security of the system. The STAR will also be used as input to the System Threats and Vulnerabilities Risk Analysis required by DoD 5200.28-M. The user, or the security expert in the PMO or SPO, should contact the intelligence function to initiate the process. See Chapter 4, "Threat Risk Management",for more details.

2.5.3.4 OPERATIONAL REQUIREMENTS DOCUMENT (ORD)

The Operational Requirements Document contains performance (operational effectiveness and suitability) and related operational parameters.

2.5.3.5 SECURE AUTOMATED INFORMATION SYSTEM REQUIREMENTS DOCUMENT (AISRD)

This document describes a required capability, justifies the need, and serves as the validation and approval document for that need. The mission user generates this document, which identifies requirements that flow from base level up the chain of command.

2.5.3.6 FUNCTIONAL DESCRIPTION

The Functional Description is also referred to as the System/Segment or "A" Specification. It is the top-level specification that describes in broad terms the operational capabilities of the system, or a major component (segment) of the system, to be acquired. The document should include macro-level functional, performance, and interface requirements that must be satisfied. The "A" Specification always answers the "what" question, and, in general, is prepared by the mission user, but may also be prepared by a support organization or contractor. Once approved, the "A" Specification becomes the functional baseline for the secure AIS.

2.5.3.7 SYSTEM/SUBSYSTEM SPECIFICATIONS

The System/Subsystem Specifications consist of a series of documents that divides and describes in more detail the specific functions and features first described by the "A" Specification. The "B" Specifications begin to further describe the design and development parameters of specific subsets of the secure AIS. Different types of these specifications include prime item, critical item, and software development specifications.

2.5.3.8 2.5.3.8 SOFTWARE UNIT SPECIFICATIONS

Software Unit Specifications are also called "C" Specifications. A detailed development specification applies to each component of the system. The "C" Specifications are the documents that the "builders" of the system use to construct the various parts of the system. Different types of "C" Specifications can exist, including critical item product specifications and software design documents.

2.5.3.9 CONTRACTING DOCUMENTS

Contracting documents are written in support of solicitations. The Federal Acquisition Regulation (FAR) provides guidance, indicates content, and sometimes provides standard formats for these documents.

2.5.3.10 INFORMATION FOR BID

This type of document is normally used for acquisitions of standard commercial off-the-shelf (COTS) items, where several vendors could provide the same item or capability. If the requirements are satisfied, the low bidder has the highest likelihood of winning the contract.

2.5.3.11 REQUEST FOR QUOTE (RFQ)

This document is a request by the Government for vendor pricing information.

2.5.3.12 REQUEST FOR INFORMATION (RFI)

This type of document typically precedes an RFP. The RFP is actually a draft RFP issued to obtain feedback from industry on the approach, content, and language of the proposed solicitation. The objective is to ensure the final RFP is clear, comprehensive, and fair to all Competitors. An RFP also helps to ensure requirements can be met using available technology, that the schedule is realistic, and the approach is workable. It is important for the Program Manager to listen to industry's feedback, although he/she does not always have to agree.

2.5.3.13 REQUEST FOR PROPOSAL

The RFP is often referred to as the solicitation package. The RFP is the most widely used document for AlS oriented acquisitions and is the focus of this procurement guideline series. The General Services Administration (GSA) has available standard solicitation documents for Systems, Software, Equipment and Maintenance. A guide on how to use these documents is also available. While the specifications for security must still be developed, the basic acquisition documents have proven to be valuable, especially to those new to acquisition. A standard RFP has thirteen sections, which are each referred to by a letter (see Table 2-1). Upon contract award, the final RFP, with sections L and M omitted, becomes the final contract guideline, including security-relevant aspects, are discussed below.

Table 2-1 RFP Organization

Letter	Section Title
A	Solicitation/Contract Form - Standard Form 33

B	Supplies or Services with Prices and Costs
C	Descriptions/Specifications/Statements of Work
D	Packaging and Marking
E	Inspection and Acceptance
F	Deliveries and Performance
G	Contract Administration Data
H	Special Contract Requirements
I	Contract Clauses
J	List of Documents, Exhibits and Other Attachments
K	Representations, Certifications and Other Statements of Offerors or Quoters
L	Instructions, Conditions, and Notices to Offerors
M	Evaluation Factors for Award

a. Section C - Descriptions/Specifications. The first part of Section C describes the mandatory technical and performance requirements to the contractor. The section is mission user-oriented, and will normally contain a Specification or Requirements section.

b. Section C - Statements of Work. The second part of Section C identifies the specific tasks the contractor will perform during the contract period. The SOW could include tasks such as design, build, test, and train. It could also require the Contractor to perform System engineering, configuration management, planning, and analysis.

c. Section H - Special Contract Requirements. This section of the solicitation contains clauses that are specially tailored for each acquisition. Typical topics covered include site access and preparation, data rights, maintenance, liquidated damages, training responsibilities, and safety.

d. Section J - List of Documents, Exhibits, and Other Attachments. This section contains a list of all documents, exhibits, attachments, and other forms used to build and execute the RFP. This section usually includes a series of attachments, each one dedicated to a list of specific items. For example, the Glossary of Terms would be one attachment, the CDRL would be another, while the list of FIPS PUBS and Federal Standards (FED STDS) would be yet another.

e. Section L - Instructions, Conditions, and Notices to Offerors. This section contains the instructions and conditions of the acquisition. It informs

Offerors of their actions and responsibilities if they submit a proposal. It covers such things as proposal format, oral presentations, and the proposal preparation instructions. Proposal preparation instructions can be used to an advantage by requiring the Offerors to submit outlines of how they will conduct SOW tasking. This process will assist in understanding the Offeror's technical approach and allow assessment of their understanding of the technical requirements.

f. Section M - Evaluation Factors for Award. This section presents to the bidder the basis of award and how proposals will be validated and evaluated. It should be taken from the evaluation team evaluation criteria (with respect to security in AISs, the topic of volume 4 of this guideline series).

2.6 REFERENCES

Although many references address the COMPUSEC acquisition process, the most important ones follow:

2.6.1 GENERAL DOCUMENTS

a. DoD Directive 5000.1, "Defense Acquisition" - Part 2 of this directive discusses integration of requirements generation, acquisition management and the PPBS (planning, programming, and budgeting system).

b. DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures" - This instruction is authorized under the direction of DoD Directive 5000.1, and is the principal acquisition directive for hardware/ software systems. The document addresses subjects like acquisition planning and management, risk management, engineering and logistics, configuration management, cost estimating, source selection, and program control.

c. DoD 5000.2-M, "Defense Acquisition Management Documentation and Reports" - This manual contains procedures and formats to be used to prepare various documents addressed in this section, including the Test and Evaluation Master Plan, the System Threat Assessment Report, Mission Need Statement, Operational Requirements, and the Life-Cycle Cost Estimate.

d. "Acquisition of Information Resources; Overview Guide," U.S. General Services Administration.

2.6.2 PLANNING AND FINANCIAL MANAGEMENT DOCUMENTS

a. DoD Directive 7740.2, "Automated Information System Strategic Planning."

b. DoD Directive 7750.5, "Management and Control of Information Requirements."

c. DoD Instruction 7041.3, "Economic Analysis and Program Evaluation for Resource Management."

d. DoD Instruction 7045.7, "Implementation of the Planning, Programming, and Budgeting System (PPBS)."

e. DoD Instruction 7045.14, "The Planning, Programming and Budgeting System (PPBS)."

f. DoD Instruction 7110.1, "DoD Budget Guidance."

g. DoD 71 10.1-M, "DoD Budget Guidance Manual."

2.6.3 CONTRACTING DOCUMENTS

a. Competition in Contracting Act of 1984 (CICA).

b. "Federal Acquisition Regulation" (FAR) and "DoD FAR Supplement."

c. "Federal Information Resources Management Regulation," (FlRMR) General Services Administration (41 CFR 201, Part 39).

d. DoD 5010.1 2-L, "Acquisition Management Systems and Data Requirements Control List."

2.6.4 PROGRAM MANAGEMENT DOCUMENTS

a. "Federal Information Resources Management Regulation," (FIRMR) General Services Administration (41 CFR 201)

b. Military Handbook (MIL-HDBK)-245B, "Preparation of Statements of Work" - This document provides guidance for preparing statements of work.

c. DoD-STD-7935A, "Automated Data Systems (ADS) Documentation Standards" - This document provides guidance for the development and revision of documentation for automated information systems. These standards apply to the documentation developed to support applications systems. This is a source for specific guidance on format and content of specifications.

d. DoD 5220.22-R, "Industrial Security Regulation" - This regulation provides uniform procedures that ensure safeguarding classified information.

e. GSA Index of Federal Specifications, Standards and Commercial Item Descriptions.

2.6.5 MISSION USER DOCUMENTS

a. "Information Systems Security Products and Services Catalogue," Prepared by the National Security Agency, (Published Quarterly) - This is the NSA publication that contains the EPL.

b. Federal Information Processing Standards Publications and Federal Standards - These two groups of Federal technical documents are also associated with most AS oriented acquisitions. The FIPS PUBS come from the National Institute of Standards and Technology (NlST) (formerly NBS); the FED STDS come from GSA. Both cover a wide range of topics. The System Engineer in the PMO or SPO should have them available and determine their specific applicability.

c. Publications issued by the Standards, Criteria, and Guidelines Division of the National Security Agency (NSA), see Appendix C, section C.t, "Working Bibliography," for a complete listing of available NCSC publications.

d. DoD Directive 3020.26, "Continuity of Operations Policies and Planning."

2.6.6 DOCUMENTS FOR BOTH PROGRAM MANAGEMENT AND MISSION USER

a. DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria."

b. DoD Directive 7920.1, "Life-Cycle Management of Automated Information Systems" - This directive specifies the six life-cycle management phases and the applicable policies.

c. DoD Instruction 7920.2, "Automated Information Systems (AIS) Life-Cycle Management Review and Milestone Approval Procedure" - This instruction defines specific tasks to be completed for each life-cycle management phase.

d. Military Standard (MIL-STD)-483A, "Configuration Management Practices for Systems, Equipment, Munitions, and Computer Software" - This military standard identifies the requirement for configuration identification, a configuration management plan, specification allocation and audits. The document addresses the relationship with other documents, reporting, configuration control, and specification maintenance.

e. MIL-STD-490A, "Specification Practices" - This standard usually applies when major systems are being acquired. This is a source of specific guidance on format and content of the specifications. Most contractor-developed documentation will follow this guideline.

f. MIL-STD-499, "Engineering Management."

g. MlL-STD-499B (Draft), "Systems Engineering."

h. MlL-H-46855, "Human Engineering Requirements for Military Systems, Equipment, and Facilities."

i. MIL-STD-1521A, "Technical Reviews and Audits for Systems, Equipments and Computer Programs. "

j. MlL-STD-1785, "System Security Engineering Program Management Requirements."

k. DoD-STD-21 67A, "Defense System Software Development."

3 COMPUTER SECURITY

3.1 INTRODUCTION

Because of its general application and the use of formal methodologies, COMPUSEC has become the most rigorous and complex of all the security disciplines. Nevertheless, a systems programming expertise is not required to understand the basic concepts. This chapter provides most of the information needed to ensure that AlS acquisitions satisfy COMPUSEC concerns.

3.2 COMPUTER SECURITY REQUIREMENTS

This section interprets requirements provided by DoD Directive 5200.28 and DoD

3.2.1 SECURITY POLICY

Security policy statements and directives form the basis for requiring security protection features in an AS. They are based on Public Laws, Executive Orders, and Federal (e.g., DoD) regulatIons. Protecting sensitive data or information from compromise, denial of service, and unauthorized alteration are fundamental requirements of DoD policy. When dealing with an AIS, the security policy can be implemented by some mixture of measures.

3.2.1.1 SECURITY PROTECTION OTHER THAN COMPUSEC

These security protection features are outside the physical or logical boundaries of the AlS. They include the physical, personnel, administrative (procedural), and operations security disciplines. External security protection measures also include the study/control of compromising emanations (TEMPEST) and communications security (COMSEC).

3.2.1.2 COMPUSEC PROTECTION

COMPUSEC protection features are inside the physical or logical boundaries of the AlS, and are emphasized in this guideline. The focus of this guideline is on computer-enforced measures, or COMPUSEC, but some overlap with the other disciplines can occur. Internal security protection measures really mean the Trusted Computing Base (TCB). The TCB is the collection of hardware, software, and procedures implemented to protect the data or information processed or stored by the AIS.

3.2.2 TRUSTED COMPUTING BASE

A TCB must be evaluated and approved to meet a set of evaluation standards.

DoD 5200.28-STD contains these standards. The four divisions of evaluation standards follow: D is minimal protection, C is discretionary protection, B is mandatory protection, and A is verified protection. C and B are further divided into two and three classes, respectively. Systems evaluated by NSA that meet a set of standards receive a TCB division/class rating. These and other systems that are evaluated for certification against the division/ class ratings are presumed to provide a degree of security protection that is "trusted" to meet the protection requirements for that division/class.

3.2.2.1 THE DIVISIONS/CLASSES

Figure 3-1 portrays the way the requirements for each class build upon preceding requirements as the division/class increases. Following Figure 3-1 are Tables 3-1 through 3-4, which cite brief definitions of each division/ class under the appropriate division heading. Note that the criteria for each division/class include and incorporate the criteria for the preceding class. The tables list the division/classes from lowest to highest confidence.

Table 3-1 Division D, Minimal Protection

There is little or no evidence of specific security protection features. (No classes exist).

Table 3-2 Division C, Discretionary Protection

Class Cl, Discretionary Security Protection - A primitive TCB provides elementary protection to separate users from data. The system is expected to operate in an environment of cooperating users processing data at the same level.

Class CS, Controlled Access Protection - A basic TCB provides intermediate-level protection. C2 features more clearly distinguish user actions through log-in procedures, auditing security-relevant events, isolating data, providing resource protection and ensuring each user is accountable.

Table 3-3 Division B, Mandator Protection

Class B1, Labeled Security Protection - An intermediate-level TCB provides elementary Mandatory Access Control protection, as well as intermediate-level Discretionary Access Control. Mandatory Access Control is extended to users and data. Data must be labeled and users must be given explicit permission to access data. Sensitivity labels are used to make access-control decisions. Such decisions are based on an informal security policy model that states the rules for how named subjects (e.g.,users) may access named objects (e.g.,files).

Class B2, Structured Protection - An enhanced-level TCB provides intermediate-level Mandatory Access Control protection and enhanced-level Discretionary Access Control. Sensitivity labels enforce access-control decisions. Decisions are based on a formally specified security policy model that regulates how every subject (e.g.,users, programs) may access every object (e.g.,files, records). Protection features are carefully separated into protection-critical and non-protection-critical elements. Class B2 requires additional internal protection, such as the prevention of information passing through covert channels. Operational support features are provided, including Information System Security Officer (ISSO) and Administrator functions. Stringent configuration management practices are required.

Class B3, Security Domains - An advanced TCB provides highly effective Discretionary and Mandatory Access Controls. B3 controls must implement the "reference monitor concept" so that all accesses are shown to satisfy a formally specified security policy model. Significant security and software engineering must be accomplished during the design, testing, and implementation phases to achieve the required level of confidence, or trust. Operational support features extend auditing capabilities, as well as ISSO functions needed for a trusted system recovery.

Table 3-4 Division A, Verified Protection

Class A1, Verified Design - A highly advanced TCB provides exceptionally effective Discretionary and Mandatory Access Controls with identical requirements to those of Class B3 TCB systems. Formal analyses prove the design and its implementation are rigorous (in the mathematical sense) using a Formal Top-Level Specification. Operational support features are further extended, providing techniques for trusted system distribution to deployed sites.

3.2.2.2 THE REQUIREMENTS

Each TCB division/class has a set of requirements. Only a general description of the protection concept appears below. No attempt is made to distinguish between divisions/classes.

3.2.2.2.1 SECURITY POLICY

Security policy statements govern the manner in which sensitive (classified) information is protected.

3.2.2.2.1.1 Discretionary Access Control (DAC) (all classes):

This is the need-to-know concept. DAC enforces rules for sharing data among users.

3.2.2.2.1.2 Object Reuse (Class C2 and above):

All storage areas (e.g., main memory or mass storage) reallocated by the system must not contain residual data for which the new subject is not authorized.

3.2.2.2.1.3 Labels (Class B1 and above):

Within a TCB, labels represent the sensitivity or security level. A subject's label represents its clearance level and need-to-know privileges; an information object's label indicates the actual sensitivity of the information. A storage object's label indicates the sensitivity of the data held or permitted to be held.

3.2.2.2.1.4 Label Integrity (Class B1 and above):

Sensitivity labels must correspond exactly to the sensitivity level of the subject (person who uses resources) or object (resources used) with which they are associated.

3.2.2.2.1.5 Exchanging Labeled Information (Class 01 and above):

Exchanging (e.g., importing or exporting) information between the TCB and a Communications channel or the TCB and a device requires the TCB to distinguish between multilevel and single-level devices.

a. Multilevel Devices (Class B1 and above): For multilevel devices, the TCB ensures that an object's sensitivity is within the range permitted. The TCB exchanges both the object and its sensitivity label.

b. Single-Level Devices (Class 01 and above): For a single-level devices, only the object needs to be exchanged. Since the sensitivity level is "fixed" and known in advance, the TCB only allows exchange at that level.

3.2.2.2.1.6 Labeling Human-Readable Output (Class B1 and above):

Output must be marked with a plain language version of the object's sensitivity level (e.g., English language security classification banner at the top and bottom of each page).

3.2.2.2.1.7 Mandatory Access Control (Class B1 and above):

From Mandatory Access Control (MAC) rules, subjects (e.g., users, programs) are allowed access (e.g., read, write, change, delete) to objects (e.g., data). A subject's clearance level must always be consistent with an object's sensitivity level. Thus, subjects may read from an area (e.g., main memory) with an equal or lesser sensitivity level, and may write to an area with an equal or greater sensitivity level.

3.2.2.2.1.8 Subject Sensitivity Labels (Class B2 and above):

During an interactive session, the TCB must keep the terminal user informed of changes in the "current working security level." Terminal users may request a display of the complete sensitivity label for processes they are using.

3.2.2.2.1.9 Device Labels (Class B2 and above):

The TCB must keep track of the minimum and maximum security level assignments of all physically attached devices (e.g,., terminals, printers). These assignments are often called "classmarks".

3.2.2.2.2 ACCOUNTABILITY

Accountability is the ability to trace actions affecting security to the responsible party. This feature ensures the user's dialogue is with the TCB and not with a masquerading program (e.g., during log-in).

3.2.2.2.2.1 Identification and Authentication (all classes):

Users must identify themselves (e.g., provide user-identifications) to the system and the TCB must authenticate the user's identity (e.g., passwords).

3.2.2.2.2.2 Audit (Class C2 and above):

The TCB must record all security- relevant events (e.g., changes to device classmarks) in a TCB-protected area called the "audit trail."

3.2.2.2.2.3 Trusted Path (Class B2 and above):

The TCB must provide a means to identify itself clearly to the user.

3.2.2.2.3 ASSURANCE

Assurance provides the steps necessary to demonstrate that the security policy has been correctly implemented.

3.2.2.2.3.1 System Architecture (all classes):

The system architecture must separate TCB processes (e.g., reference monitor) from user processes (e.g., application programs). The system architecture must also separate each user's data from every other user's data.

3.2.2.2.3.2 System Integrity (all classes):

Periodic validation checks must ensure the correct functioning of the TCB protection elements. The checks can either be automated, or they can be invoked manually by the system operator.

3.2.2.2.3.3 Covert Channel Analysis (Class B2 and above):

Covert channels are signalling paths that can bypass the TCB's access controls and therefore, can allow violation of policy. Covert channels must be identified, their bandwidth minimized, and their use audited.

3.2.2.2.3.4 Trusted Facility Management (Class B2 and above):

The separate functions of system operator and system administrator must be defined and supported with TCB features. The system operator has fewer security-relevant privileges than the system administrator.

3.2.2.2.3.5 Security Testing (all classes):

The range and depth of testing increases for each division/class. Test results must affirm the implementation of security protection features as intended.

3.2.2.2.3.6 Design Specification and Verification (Class B1 and above):

The security policy enforced by the TCB must be informally (i.e., non-mathematically) struCtured or formally (i.e., mathematically) modeled. At higher TCB classes, the mathematical modeling becomes more rigorous (e.g., the spectrum includes demonstration, providing a Convincing argument, and proving). The requirement for correspondence between the policy model and the design specifications (e.g., Descriptive Top-Level Specification (DTLS) and Formal Top-Level Specification (FTLS)) also increases.

3.2.2.2.3.7 Configuration Management (Class B2 and above):

Configuration management refers to the procedures used to establish a baseline and then to control changes throughout the system's life cycle. Configuration management becomes more comprehensive as the TCB division/ class increases.

3.2.2.2.3.8 Trusted Recovery (Class B3 and above):

Procedures must be available to preserve seCurity protection integrity and return the system to a secure processing environment after a failure.

3.2.2.2.3.9 Trusted Distribution (Class A1):

This feature ensures the provision of a "high confidence" system for distributing each TCB version, also ensuring its integrity upon receipt at each site.

3.2.2.2.4 DOCUMENTATION

The documents required describe the TCB's objectives, design, performance, and operation. Documentation must include a Statement of Work task to develop these documents and invoke the Contract Requirements Lists (CDRLs) to specify delivery to the Government.

3.2.2.2.4.1 Security Features User's Guide (all classes):

This guide targets system users and developers. The document describes the security protection features of the TCB, provides guidelines on their use, and explains how they interact. The guide should also describe expected system reaction to security-relevant events, such as access violations.

3.2.2.2.4.2 Trusted Facility Manual (all classes):

This manual applies to the System Administrator, Security Officer, users, and operators. Since this document provides detailed information about the security protection features provided by the TCB and describes how to use them, its distribution should be strictly controlled. The document should cover "everything you need to know" to generate and operate the specific TCB in an operationally secure environment. This information should include loading, generating, and initializing a new TCB; maintaining and examining audit files; conducting shutdown, restart, and recovery; as well as running diagnostics, managing sensitivity labels, and managing user access authorizations.

3.2.2.2.4.3 Test Documentation (all classes):

Test documentation provides the test plan(s) and the results of testing the TCB security protection features. The range and depth increases as the TCB division/class increases. Test results must be controlled if they point out vulnerabilities.

3.2.2.2.4.4 Design Documentation (all classes):

A full complement of design documentation is required. The scope depends on the TCB division/class. The scope ranges from a simple statement of the protection objectives through a mathematically based description, to the detailed proofs and correspondence of the specifications, and back to the security policy model and its objectives.

3.3 SOFTWARE

Since most computer security protection features are implemented in software, a clear majority of the Program Manager's time is spent dealing with software issues. Time should be taken to review DoD 5200.28-STD as well as the other references given at the end of this chapter. This review will help the Program Manager prepare for the acquisition concerns about software.

3.3.1 PRINCIPAL SOFTWARE FACTORS

This section identifies software factors important in a trusted application.

3.3.1.1 STRUCTURE AND DISCIPLINE

Software matters require structure and discipline. Structure provides procedures, techniques, and check-points used to measure progress. Detailed planning, step-by-step execution of the plans, and an iterative approach are important. Discipline provides a way to remain on the charted course without being trapped by pitfalls. One must do more than blindly "follow the rules." Good documentation configuration management, and strict adherence to details are important discipline factors.

3.3.1.2 COST ESTIMATING

Estimating the cost of software development is difficult, at best. Cost overruns invariably lead to increased software risk, a serious concern for secure systems. Tools are available that contractors and other software developers use for cost estimation. Nevertheless, a great deal of subjective input influences to the "final" estimate. The skill level of the people involved, the complexity of the system, and many other factors all play a role. The contractor must describe the process, ground rules, and assumptions used to estimate software development costs. The Program Manager should "walk through" the steps to be certain the process makes sense. If the contractor's documentation cannot be fully understood, he/she should be asked for an informal briefing or chalk-board session. This process may avoid major cost and schedule changes later.

3.3.1.3 PROGRAMMING LANGUAGE

An appropriate modern, high-order programming language should be required to improve security. For example modern languages that strictly enforce "strong typing" should be used. Strong typing is the assignment of legal access (e.g., read, write, modify) to objects. Moreover, languages often require programmers to restrict their data definitions to pre-designated storage areas (e.g., certain main memory blocks). Ada is the DoD required language, and alternate languages must be preapproved. Software engineering disciplines (structured programming with structured "walkthroughs") make it more difficult for an attacker to hide covert code or logic bombs. If the use of assembly language for applications is allowed, the source must be checked carefully for illegal Operations (e.g., the use of undocumented operations codes). Such use would require a special section in the test plans and configuration management plan.

3.3.1.4 DATABASE MANAGEMENT SYSTEMS (DBMSs)

Systems that use DBMSs can introduce an additional element of risk not present in non-DBMSs. NCSC-TG-021, "Trusted Database Management System Interpretation of Trusted Computer System Evaluation Criteria," provides criteria for dealing with this important issue.

3.3.1.5 UTILITIES

System utilities provide powerful tools for augmenting or developing operating system capabilities. Their use must be limited and controlled by the TCB software. The security implications for compilers that "automatically optimize" the generated object code must be understood. That is, the generated object code will likely not be in the identical sequence Corresponding to the source language, although the function performed will be correctly done. Linkers (sometimes called "Linkage Editors") can also be a security concern, since access to unintended data areas can Occur through "external reference" directives. Finally, some languages incorporate what is known as "run-time packages," chiefly to perform input-output operations. Run-time packages must be included within the security-relevant boundary, especially at the higher TCB divisions/classes.

3.3.2 THE PROCESS

Figure 3-2 illustrates the software development process in terms of documentation required. Different terms are used for some of the design documents, but the document requirements are similar, if not identical. For example, the terms Functional Description, "A" Specification, and System Specification, are usually used interchangeably. Note that the process is iterative, and flows from very general top-level policy and capabilities requirements statements, down to very precise implementation details.

```
               Security Policy
                      *
             Security Policy Model
                      *
            Functional Description
              ("A" Specifications
     Descriptive Top Level Specification (DTLS)
   Formal Top Level Specification (FTLS, A1 only))
                      *
         System/Subsystem Specifications
              ("B" Specification)
                      *
              Unit Specifications
              ("C" Specification)
```

Figure 3-2 Security Protection in the Software Development Process

3.3.3 MANAGING SOFTWARE DEVELOPMENT

As noted above, the key to success with software is structure and discipline. Some of the specific success factors follow:

3.3.3.1 DESIGN DOCUMENTATION

Documentation must start from the initial statement of requirements and continue through to the details of implementing, operating, and maintaining the system. The root is in the initial statement of requirements.

3.3.3.1.1 SECURITY POLICY

An explicit statement of the security policy should be enforced by the AS. The policy should be documented in the specification (requirements) section of the RFP, and should clearly state the security enforcement rules by which the system will operate.

3.3.3.1.2 MODEL

Each TCB division/class requires a vendor or manufacturer (i.e., contractor) to provide a description of the security protection philosophy and how that philosophy is translated into the TCB. TCB Class B1 requires development of an informal or formal description of the security policy to be enforced by the TCB. TCB Class B2 and above require formal models of the security policy. As might be expected, these models (both informal and formal) require special expertise to develop and evaluate, since they will be written in special mathematical notation (e.g., algebraic specification or set theory). It should be ensured that the expertise needed to review and evaluate the contractor's submissions is available, either internally or from the NSA.

3.3.3.1.3 DESCRIPTIVE TOP-LEVEL SPECIFICATION

The DTLS is equivalent to a Security Features Functional Description. This specification describes the security protection capabilities required by the AIS, and is required for TCB Classes B2, B3, and A1. Although written in English prose, this document will contain a good deal of technical language. The DTLS should address both hardware and software capabilities.

3.3.3.1.4 FORMAL TOP-LEVEL SPECIFICATION

This document is required for TCB Class A1 only. It is written in a formal mathematical language to ensure that the design is consistent with the model of the security policy being enforced. The FTLS also addresses both hardware and software protection. This specification is accompanied by a separate formal verification of the specification. This verification proves that the design corresponds completely and accurately to the formal security policy model. Special expertise is also required to review and evaluate this document.

3.3.3.1.5 SYSTEM/SUBSYSTEM SPECIFICATION ("B" SPECIFICATION) AND UNIT SPECIFICATION ("C" SPECIFICATION)

The design documentation, from this level down, begins to describe, in ever-increasing detail, the "how-to" of the TCB build process. At this level of detail, care must be taken when reviewing the contractor's design approach. Concern should focus on thoroughness and completeness, not "how to." If the required capabilities, functions, and features are present, the contractor should have some freedom of choice. The contractor must also comply with the contract-specified standards and specifications. If a question arises as to what the document is saying, the program manager should ask for an informal briefing or chalk-board session.

3.3.3.2 PROGRAMMING

Programming, or writing computer programs, is the "build" of the development process. The contractor should not begin to program until after approval of the specifications. This restriction will avoid restarts and changes as the acquisition progresses.

3.3.3.3 TESTING

Both the contractor and the Government are heavily involved in testing. The attitude should be "Show me, please" throughout the test effort. For the internal TCB-provided security protection features, DoD 5200.28-STD requirements should be reviewed for testing each division/class. A team of experts should be assembled to help test. Also, Chapter 5 of this document, "Security Test and Evaluation," should be reviewed.

3.3.3.4 CONFIGURATION MANAGEMENT

Configuration Management (CM) for TCB software is only required for TCB Classes B2 and above. However, CM should be required for all acquisitions, whenever possible. CM is the only way to achieve a structured and disciplined approach to software management, regardless of the TCB division/ class. The situation is likely that some CM will be required in every program. The requirement extends to the TCB software by including a Statement of Work task. The Program Manager should also participate in the Configuration Control Board (CCB), which is the committee that reviews all changes to established baselines. Note that the documented procedures for control of changes do not need to be as extensive for the lower TCB division/classes (C1 through B1). Configuration control must extend to distribution, delivery, installation, Operation, and maintenance.

3.3.3.5 AUDIT

Auditing of security-relevant events is required for all TCB division/ classes (C2 and above). The early identification of audit requirements and strategy is necessary to ensure that the accountability requirements are satisfied for the TCB division/class, and to ensure they are included in the TCB design. The NSA publication NCSC-TG-001,"A Guide To Understanding Audit In Trusted Systems," describes the specific audit requirements for each TCB division/class, including the events that must be audited and the specific information that must be recorded.

3.3.3.6 PASSWORD GENERATION AND MANAGEMENT

One of the major requirements of all TCB division/classes is accountability. The CSC-STD-002-85, "DoD Password Management Guideline," and NCSC-TG-017, "A Guide to Understanding Identification and Authentication," provide sound practices that will help satisfy the accountability requirement. Ensure accountability is included in all AIS RFP requirements. Also ensure the information provided in the Trusted Facility Manual and Security Features User's Guide is consistent with the principles in this guideline.

3.3.3.7 TCB IMPLEMENTATION CORRESPONDENCE

The process of assuring that the TCB is "properly done" is called "correspondence." The technique used is to map the TCB design back to the security policy model at the B1 and above levels. In addition, the TCB Class A1 requirement calls for mapping the TCB design down to the TCB source code.

3.3.4 CLASSIFIED SOFTWARE

If any of the software being developed is classified, be sure to check Block 11c, Receipt and Generation of Classified Documents and Other Material, of the DD Form 254, Contract Security Classification Specification. Trusted software must be protected at the highest level of information to be processed.

3.3.5 ACQUISITION TASKS

To ensure a structured and disciplined approach to software concerns, provide Statement of Work tasks appropriate for the TCB division/class being developed.

3.4 HARDWARE

Several features of a TCB have an impact on hardware or require hardware for support.

3.4.1 PRINCIPAL HARDWARE FACTORS

This section identifies factors associated with hardware that are important in a trusted appliCation.

3.4.1.1 INITIAL PROGRAM LOAD (IPL)

Sometimes referred to as "boot" or "bootstrap," the IPL function is always hardware based. The IPL feature loads and begins executing the first few instructions necessary to start the system. The chief security concern is the initial secure state for TCB Classes B2, B3, and A1. Without assurance the system achieves the initial secure state, the TCB cannot be considered secure.

3.4.1.2 PROCESSOR STATES

To be suitable for a TCB, a computer must have at least two distinct processor states (sometimes referred to as "operating modes"). The most privileged state should be reserved exclusively for the TCB's use and should include special instructions or features needed to enforce access control rules or perform input/output functions. Another, less privileged state should be used by the application programs and must not include those powerful security-related capabilities reserved for the TCB. The idea is to isolate privileged capabilities and restrict the use of certain instructions (e.g., those which do input/output or enforce access control rules) to the TCB alone, while permitting the applications programs to perform their mission-oriented functions at a less privileged level.

3.4.1.3 PROTECTION DOMAIN GRANULARITY

Small domains (e.g., a few bytes) are ideal for providing precise control (down to the byte or word level) but they require a significant amount of computer overhead to maintain. The trade-off usually made is to have larger protection domains (e.g., 1024 byte blocks) to reduce hardware complexity and retain acceptable performance.

3.4.1.4 SENSITIVITY LABEL MAPPING TO PROTECTION DOMAIN

MECHANISMS

Hardware features (usually called "keys") allow the TCB to associate specific hardware "registers" with the main memory areas (domains) they are protecting. There should be sufficient types and numbers of "registers" to ensure the number of sensitivity labels for information in the system can be adequately mapped. Common ways to achieve these capabilities are through "Descriptor Base Registers," "Bounds Registers," and "Virtual Memory Mapping Registers," although other approaches may also be used.

3.4.1.5 INTEGRITY CHECKING MECHANISMS

Integrity checking mechanisms usually provide support for security functions. For example, memory parity checks and cyclic redundancy check schemes ensure errors are detected. Another commonly used technique is called a watchdog timer. This timer performs a direct security-related function by ensuring an application program cannot "steal all the processor's time" by independently checking allocations of processor time.

3.4.1.6 DIRECT MEMORY ACCESS (DMA) PROTECTION

DMA allows input-output to occur simultaneously with the processor's normal computational activities. That is, once the processor initiates an input-output operation, a separate hardware feature directs the flow of data into (or out of) main memory independent of the processor, while the processor itself is free to complete other tasks. Since DMA is independent of processor intervention, it cannot be confined by the TCB's enforcement techniques. Thus, unless DMA security protection is provided, Mandatory Access Controls cannot be enforced during DMA operations.

3.4.1.7 ASYNCHRONOUS EVENT MECHANISMS

Asynchronous events are not predictable (e.g., arrival of a message, the printer's running out of paper, or communications link errors). Asynchronous event mechanisms are hardware features which handle the unpredictable, usually by "interrupting" the processor. Once interrupted, the processor then deals with the event. For security, the hardware features should cause the processor to recognize and respond to specific asynchronous events, such as "security policy violations" (in DoD 5200.28-STD phrasing, violations of the Simple Security Property or Star Property). Unless hardware features support these properties, software must interpret the results of every operation, -causIng a severe performance penalty. The penalty may come into conflict with mission performance requirements.

3.4.2 CAVEATS

Care must be taken not to restrict potentially valid solutions in the specifications (requirements), statement of work, or CDRL sections of the RFP. Many possible design solutions could meet the requirements. Use of specific terms could unintentionally preclude the application of alternative techniques. Thus, terms should be used that illustrate the concepts involved without restricting the design choices available to the contractor. The second guideline of this four-guideline series, "Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators," was written specifically to deal with this problem.

3.4.3 MANAGING HARDWARE

Dealing effectively with security-relevant hardware issues follows the same general process as for software. Some specific points to consider include the following:

3.4.3.1 IDENTIFY SECURITY PROTECTION FUNCTIONS

The Program Manager (or the contractor) should trace the allocation of system functions, that are hardware based, from requirements to specific devices in the "as-built" drawings. In this way, the hundreds of design choices made should not neglect hardware issues, especially where specific hardware support is needed for the Trusted Computing Base.

3.4.3.1.1 SECURITY PROTECTION CAPABILITIES

Security protection capabilities are identified in the top-level specifications. Security protection features allocated to hardware may be found in the hardware section of the Functional Description or Descriptive Top-Level Specification.

3.4.3.1.2 HARDWARE INFORMATION

Hardware information will exist in most of the "B" and "C" Specification software design documents. This information should allow tracing hardware security protection features to successively lower levels of detail.

3.4.3.1.3 SPECIFIC DETAILS ON THE HARDWARE FEATURES

Details in Section 3.4.1.6 (e.g., DMA protection) can be found in the engineering data deliverables. Ensure the Contractor provides the technical data and drawings needed to assess the hardware.

3.4.3.2 CONFIGURATION MANAGEMENT, MAINTENANCE, AND

LIFE-CYCLE SUPPORT

These functional areas should follow the same general approaches taken for other security-related functions.

3.5 NETWORKS

Network security may be a major issue, but many aspects are beyond the scope of this guideline. Guidance for network security may be found in NCSC-TG-005, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria." If significant networking requirements exist, issues should be addressed early. Be prepared to face difficult problems early in the program.

3.6 COVERT CHANNELS

A covert channel provides a means of Communicating information in a way that violates the security policy. The two types of covert channels are storage and timing. A storage channel occurs when a "sending" process stores an item of data and a "receiving" process detects and interprets the information covertly. A timing channel occurs when a "sending" process affects a timedependent system parameter, and a "receiving" process observes and interprets this effect as a bit of information.

3.6.1 DETECTION

Covert channels are easy to hypothesize, but difficult to detect, and often they cannot be totally eliminated. The next-best approach is to try to identify them, reduce their effectiveness, and provide a measure of control over them. Execution flow analysis can sometimes detect storage channels, but no formal methods can detect timing channels at this time.

3.6.2 RATES

High covert channel transfer rates (over 100 bits/sec) are a major concern and are generally unacceptable. Low transfer rates (under 1 bit/sec) are of less concern because it would take too long to Communicate significant amounts of information. (It cannot be forgotten, however, there are situations in which a single number or name can be highly classified.) Intermediate transfer rates introduce the need for the ISSO to monitor covert channel activity. This procedure is done by auditing all known events that may be used to exploit the covert channel. The Trusted Facility Manual should contain information on what events are audited and how they should be interpreted.

3.6.3 COVERT CHANNEL ANALYSIS

A covert channel analysis is required for Classes B2, B3, and A1. In acquisitions requiring these classes, a Statement of Work task should be included in the RFP that requires the contractor to conduct a covert channel analysis and the CDRL that lists the development of a Covert Channel Analysis. This process will require the contractor to deliver a technical report to the Government that documents the results of the analysis. An assessment of the report will reveal whether covert channels are sufficient to cause redesign or can be tolerated by using auditing techniques.

3.7 MAGNETIC REMANENCE

The retentive properties of magnetic storage media and the known risks in erasing and releasing such media should be considered in all AIS acquisitions. The correct procedures for clearing and declassifying AS magnetic media must be included in the design and implementation documentation of ASs. Contractor and Government personnel must both use NSA-approved standards for degaussing and overwriting. Degaussing equipment must be evaluated and approved to meet the standards. Auditing, record-keeping, testing and control of overwrite software, and the handling of equipment malfunctions are risk areas that are often neglected.

3.7.1 GUIDELINES

NCSC-TG-025, "A Guide to Understanding Data Remanence in Automated Information Systems," should be included in all RFP requirements. Another excellent source document is Defense Intelligence Agency Manual 50-4, "Security of Compartmented Computer Operations(U)," CONFIDENTIAL.

3.7.2 REQUIREMENTS

Whenever possible, the hardware specifications should require that solid-state data storage components be volatile (i.e., total clearing of data with power off). Exceptions (e.g., plated wire memory used for extremely high reliability applications) require other protection approaches.

3.7.3 MAINTENANCE

The maintenance concept for the AS must address the magnetic media remanence issue. In particular, the Trusted Facility Manual should include procedures for clearing and sanitizing magnetic storage media. Dial-in diagnostics, warranty repairs requiring shipment of the component back to the contractor, and disposition of replaced components are areas for special consideration. In addition, if non-volatile devices are used, they must be clearly identified (and labeled if possible).

3.7.4 DECLASSIFICATION AND DESTRUCTION

Procedures should be available that address clearing and declassifying AIS equipment and media. Clearing is a procedure that removes the classified information recorded on the media, but cannot totally declassify the media. Declassification is a procedure that totally removes all classified information recorded on magnetic media. The declassification method should be used when equipment or magnetic media are to be removed from the AIS or a controlled environment.

3.8 RATIONALE FOR SINGLE-ENTITY APPROACH

This section provides rationale for limiting the scope of this document to single-entity systems, as was reflected in Paragraph 1.5.

3.8.1 INTERPRETING THE ORANGE BOOK

The second page of the TCSEC states: "This document is used to provide a basis for specifying security requirements in acquisition specifications." This does not mean one can combine one Class C2 requirement with four Class B3 requirements. Implicit to the statement is the division/class structure. For a defined entity of a system to be guaranteed secure in the Orange Book sense means that, at a minimum, all of the requirements of some identified division/class must be met. To Call that entity a Class B2 entity, however, would require evaluation by NSA as a product satisfying the Class B2 criteria. A successful certification evaluation of an entity can only state that evaluation and approval have been completed as part of a Certification process against, at a minimum, the Class B2 set of requirements. Nevertheless, that does not make the resulting system Class "B2."

3.8.2 PROCUREMENT CONSTRAINTS

In a procurement, the RFP cannot dictate that an item must appear in the EPL because of the limited number of items on the EPL, and because the process for placement on the EPL is itself a restricted, government controlled process. To state such a requirement in the RFP would constitute a discrimination against other vendors desiring to bid. It also can not be stated that "a B2 system is required" because that implies a product must be taken from the EPL.

Therefore, the specific TCSEC requirements necessary to meet a Certain division/class rating must be identified, without stating that the B2 product is desired. The desire for the decreased risk normally inherent in an EPL product, however, can and should be reflected as a strong evaluation weighting factor for source selection.

3.8.3 MULTIPLE-ENTITY SYSTEMS

A system may be composed of two or more entities, each of which uses different division/class security requirements. Some examples of the rationale for doing this are provided in NCSC-TG-021,"Trusted Database Management Interpretation" and also in Appendix A of NCSC-TG-00s, "Trusted Network Interpretation." The reason could also be that, as a system evolves, a higher level of security may be mandated for a new part (entity) of the system (called "Y") than was mandated for the existing entity (called "X"). Rebuilding the entire system is often not practical. The alternative is to consider X and Y as distinct connected entities.

3.8.3.1 ENTITY PROTECTION

Distinct connected entities X and Y must be isolated from one another in a security sense. They each must meet their distinct security requirements. Communications by each to the other must be shown to meet an interface policy given for each. The interface policy must reflect the outgoing/incoming security policies, mutual trust, cascading effect, and least privilege considerations. If additional security requirements above those from the TCSEC have been imposed (e.g., a two-person rule), these requirements must be considered in the interface policy.

3.8.3.2 ENTITIES WITH THE SAME DIVISION/CLASS

Even two connected B3 systems may have to be treated as distinct entities. One B3 system may have resulted from an uncleared minimum user clearance with maximum Secret data sensitivity and the other B3 system may have resulted from a Confidential minimum user clearance and maximum Top Secret data sensitivity (see Enclosure 4 of DoD Directive 5200.28). Cascading risk would probably require the combined system to be evaluated using Class A1 criteria.

3.8.4 RECOMMENDATIONS

As stated before, this set of four acquisition documents does not deal with this complicated situation of acquiring multiple security entity systems because DoD policy has not been finalized. This document series only deals with single system-entities. Successfully evaluated products will be said to "possess" a division/class (e.g., Class B3). System entities will be said to require some minimum division/class level (e.g., Class B3) requirements. System entities having successfully passed certification evaluation against a minimum division/class set of requirements will be identified, but those entities cannot be called, for example, Class B3 entities or systems. Instead, use "B3" for Class B3-evaluated products and "systems (or system entities) certified against Class B3 requirements" for the cases treated in this document set.

3.8.5 WHAT TO DO IN THE MEANTIME

As soon as composition and interface policy mature to a viable status, this document set will be updated. In the meantime, for Program Managers faced with the more complicated situations not dealt with in this series, the above principles can be extrapolated, along with discussion and interpretation in the TNI and TDI, as guidance.

3.9 REFERENCES

Many reference documents apply to a Trusted Computing Base acquisitions. Some address only COMPUSEC. Others address all security disciplines, all software development, or development of an entire system. Each document must be considered for COMPUSEC in the context of the intended scope. The following documents should be available.

a. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)" - This Directive applies to all automated information systems processing classified, sensitive unclassified, or unclassified information. The document specifies the applicability of DoD 5200.28-STD (the Orange Book). It also specifies that systems requiring at least controlled (C2) access based on the risk assessment procedure (i.e., not all users necessarily have the need to know for all information) must be upgraded by 1992.

b. DoD 5200.28-M, "Automated Information System Security Manual" (Draft) - This manual specifies AlS security officer roles and responsibilities, risk management, certification and accreditation requirements, and security policy requirements. This document also addresses provisions of the Computer Security Act of 1987.

c. DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria" - The "Orange Book" contains a set of basic requirements and evaluation criteria for assessing the effectiveness of security protection features provided to an automated information system.

d. DoD-STD-7935A, "Automated Information System (AIS) Documentation Standards" - This standard provides guidelines for the development and revision of documentation for an automated information system or applications software. The document specifies the content of each of the eleven types of documents that may be produced during the system's life-cycle.

e. DoD-STD-21 67A, "Defense System Software Development" - This standard establishes uniform requirements for software development applicable throughout the system life-cycle. The document identifies the software development process and discusses deliverable products, reviews, audits, and baselines.

f. CSC-STD-002-85, "Department of Defense Password Management Guideline" - This standard presents a set of suggested practices for designing, implementing, and using passwords in automated information systems that process sensitive information.

g. CSC-STD-003-85, "Computer Security Requirements - Guidance for Applying Department of Defense Trusted Computer System Evaluation Criteria in

Specific Environments" - This Document identifies the minimum recommended Trusted Computing Base division/classes required for given risk indices. This standard illustrates the rating scales for minimum user clearance and maximum data sensitivity, and then shows the resultant TCB division/class based on the computed risk index and security mode of operation. Parts of this document were incorporated in enclosure 4 of DoD Directive 5200.28 with slight modifications and interpretations. Therefore the directive should be used for risk indices.

h. CSC-STD-004-85, "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments" - This document provides background information and a more detailed explanation of the recommended minimum TCB division/classes for given risk indices.

i. NCSC-TG-001, "A Guide to Understanding Audit in Trusted Systems" - This guide expands on and clarifies the concept of audit as presented in DoD 5200.28- STD.

j. NCSC-TG-003, "A Guide to Understanding Discretionary Access Control in Trusted Systems" - This guide expands on and clarifies the Concept of discretionary access control as presented in DoD 5200.28-STD.

k. NCSC-TG-005, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria" - This basic document interprets and augments DoD 5200.28-STD for network applications.

l. NCSC-TG-006, "A Guide to Understanding Configuration Management in Trusted Systems" - This guide is a key document in the secure system development process.

m. NCSC-TG-009, "Computer Security Subsystem Interpretation" - This document interprets DoD 5200.28-STD for dealing with subsystems of secure Systems.

n. NCSC-TG-014, "Guidelines for Formal Verification Systems" - This guideline expands on and clarifies the use of formal verification as presented in DoD 5200.28-STD.

o. NCSC-TG-015, "A Guide to Understanding Trusted Facility Management" - This document is useful in writing the Trusted Facility Manual.

p. NCSC-TG-017, "A Guide to Understanding Identification and Authentication in Trusted Systems" - This document presents good practices related to trusted identification and authentication.

q. NCSC-TG-021, "Trusted Database Management System Interpretation of Trusted Computer System Evaluation Criteria" - This document interprets and augments DoD 5200.28-STD for database management systems. This interpretation also addresses TCB subsets and the evaluation of systems built out of parts, for example, sold by different vendors.

r. NCSC-TG-025, "A Guide to Understanding Data Remanence in Automated Information Systems" - This document provides guidance and procedures on clearing and declassifying automated information system magnetic storage media such as memory, tapes, disk(ette)s, drums, and cassettes.

s. NCSC-TG-026, "A Guide to Writing the Security Features User's Guide" - This document provides guidance in writing the important Security Features User's Guide

t. FIPS PUB 83, "Guideline for User Authentication Techniques for Computer Network Access" - This document provides a thorough treatment of the user authentication as applicable to computer networks.

u. FIPS PUB 112, "Password Usage Standard" - This is a good source document for the specification and management of passwords.

v. FIPS PUB 113, "Computer Data Authentication" - This document deals with authenticating computer data.

w. ISO 7498/Part 2, "Security Architecture" - This specification was developed for use with the Open Systems Interconnection (OSI) network model.

x. Gasser, M., "Building a Secure Computer System" - This book provides an understandable technical presentation of the many aspects of securing computer systems. This book provides information about proven methods and affords the reader a broad understanding of COMPUSEC terms, concepts, problems, and solutions.

4 THREAT RISK MANAGEMENT - ANALYSIS, DESIGN, AND IMPLEMENTATION

4.1 INTRODUCTION

DoD Directive 5000.1 states "risk areas . . . to be assessed shall include threat, technology, design and engineering, support, manufacturing, cost, schedule, and concurrency." Program management must deal with each risk. However, when a computer security person is asked about risk, the primary concern is the threat risk of someone inadvertently or purposely obtaining, altering, or destroying classified or sensitive information in an unauthorized manner. Threat risk is sometimes called "security risk." That is the risk addressed in this chapter.

Risk management is the total process used to identify threat risks and eliminate or reduce them to acceptable levels. The components of threat risk management are risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and Systems review. This chapter covers risk management during analysis design and implementation. Chapter 5 deals with security test and evaluation. Chapter 6 describes the activities involved in obtaining certification and accreditation.

4.2 SECURITY REQUIREMENTS

Although people usually do not consider requirement definition as a security risk management function, security risk management is very much involved in the requirement definition process. Part of the risk management function, under the auspices of the Designated Approving Authority (DAA), is to determine how the regulatory requirements, embodied in DoD 5200 series of documents, are satisfied in this particular application. The approach to satisfying these requirements (such as the assignment of maximum data security and minimum clearance levels) helps to dictate the operational security (OPSEC) requirements. Those requirements are determined through analysis of cost, risk, and mission considerations.

4.2.1 DOCUMENTING SECURITY REQUIREMENTS

DoD Directive 5200.28 requires "a more accurate specification of overall DoD security requirements." The security aspects of the plans required under DoD Instruction 5000.2 (Part 11E) should be combined into a single document, the Systems Security Plan. A portion of the concept baseline documentation called for in the Concept Exploration and Definition Phase (Parts 3 and 4B) should be described in the System Security Concept of Operations. This process is consistent with the concept of isolating the security process to help achieve a higher level of assurance.

4.2.2 SYSTEM SECURITY PLAN

The SSP describes the system security engineering program. This document describes methods to identify security requirements, evaluate and synthesize proposed solutions, and coordinate security considerations and requirements with the other functional areas in the system development process. The SSP also describes the organizational structure, staffing, and other resources that will be allocated to satisfy security requirements. The SSP is a living document and must be updated as change occurs.

4.2.3 SECURITY POLICY

Security policy statements are always the basis for requiring security protection features in an AIS. The two basic sources of security policy are regulatory and operational.

4.2.3.1 REGULATORY

Regulatory seCurity policies are based on Public Laws, Executive Orders, and the many Federal and DoD regulations. The protection of sensitive data from compromise, denial of service, or unauthorized alteration is the fundamental requirement of national security policy.

4.2.3.2 OPERATIONAL

Operational policy specifies the operational approach taken to satisfy the regulatory policy as well as any additional operational security requirements. High-level operational policy involves decisions across all aspects of protection, including software and hardware functions, administrative procedures, personnel clearances and physical security measures. Risk assessment achieves the next level of requirements, which include operational classifications and clearances, security mode, and the COMPUSEC division/class requirements. Other mission-specific security requirements, or operational constraints that impact security, must be specified as policy. Operational policy may further evolve based on risk analysis, cost/ benefit analysis, and even safeguard design decisions.

4.2.4 SYSTEM SECURITY CONCEPT OF OPERATIONS (SSCONOPS)

The SSCONOPS is an architectural-level document that defines the strategy for meeting both operational and regulatory policy requirements. A secondary intent is to develop a comprehensive document that provides architectural-level direction for the total system security approach. Thus, the SSCONOPS serves as the model for security planning and execution for other parts of the program.

4.2.5 ACQUISITION SYSTEM PROTECTION PROGRAM (ASPP)

The ASPP is under development by the Office of the Director of Defense Research and Engineering. It will provide an orchestrated DoD program to identify critical technologies and to provide techniques, procedures, and personnel necessary to deny foreign collection efforts involving those technologies.

4.3 RISK ASSESSMENT

Risk assessment is a procedure to determine the minimum evaluation division/class requirement for an AIS based on the sensitivity of the information present and the clearances of its users. Risk assessment is usually performed during the concept development phase, prior to system design. This process determines the security mode to be employed and an evaluation division/class.

4.3.1 RISK INDEX

Risk Index represents the disparity between the minimum clearance or authorization of AlS users and the maximum sensitivity (e.g., classification and categories) of data handled by the AlS. The Risk Index "computes" the approximate degree of security protection features required for an AlS application. DoD Directive 5200.28, Enclosure 4, provides instructions for the computation, as follows:

4.3.1.1 DATA SENSITIVITY

The sensitivity of data can range from "Unclassified" through "Top Secret with two or more categories." Each level of data sensitivity is assigned a number rating ranging from zero to seven.

4.3.1.2 USER CLEARANCE

The people who will use a system can have security clearances ranging from "Uncleared" to "Top Secret with Multiple Categories". Each level of security clearance is also assigned a number rating ranging from zero to seven.

4.3.1.3 REQUIRED TRUSTED COMPUTING BASE

The required TCB is determined by subtracting the user clearance rating from the data sensitivity rating. The result is the Risk Index (a number ranging from zero to seven). The Risk Index is then found in a table that prescribes the corresponding minimum-required TCB division/class and security mode combination. The security mode and minimum security division/class requirements are given in Table 4-1. As one moves down the table, increasing reliance is placed on the TCB Operating system to provide security protection features. Also, the cost of the TCB goes up and operational flexibility increases, in terms of who can use the system.

Table 4-1 Security Modes and Minimum Division/Class

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

(* Beyond the state of current computer technology)

4.3.2 SECURITY MODE OF OPERATION

A security mode of operation describes the environment under which sensitive information is processed. DoD Directive 5200.28 defines four security modes of operation. Some agencies and applications define modes to a finer granularity. Nevertheless, all must satisfy these basic requirements.

4.3.2.1 DEDICATED SECURITY MODE

Each user has the clearance, authorization, and need-to-know for all data handled by the AlS. If the AIS processes special access information, all users require formal access approval. An AS may handle a single classification level and/or Category of information or a range of levels and categories. In the latter, there is heavy reliance on externally provided security protection features, such as security downgrade guards, if any stored information is to be treated at a level lower than the processing.

4.3.2.2 SYSTEM HIGH SECURITY MODE

All users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval. Again, there is heavy reliance on externally provided security protection features, such as security downgrade guards, if any stored information is to be treated at a level lower than the processing.

4.3.2.3 PARTITIONED SECURITY MODE

All personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the AlS. This security mode encompasses the compartmented mode defined in DClD 1/16. There is a heavy reliance on both internally and externally provided security protection features.

4.3.2.4 MULTILEVEL SECURITY MODE

The multilevel security mode allows two or more classification levels of information to be processed simultaneously within the same system, when not all users have a clearance or formal access approval for all data handled by the AIS. These controls are applied in varying degrees, depending on the sensitivity of the information and the users' clearances.

4.4 COST/BENEFIT ANALYSIS

The Cost Benefit Analysis helps to ensure that the security protection features selected for an AIS are cost effective. Nevertheless, this does not mean "low-dollar" or least expensive. The selected countermeasures must be effective, provide a measure of utility, overlap other countermeasures where possible, and have reasonable costs. Although cost benefit analysis is identified as a risk management function in DoD Directive 5200.28, further discussion about the subject may not be found elsewhere in regulatory security documentation. Security is achieved by a combination of software and hardware functions, administrative procedures, personnel clearances, and physical security measures. The DAA determines the required balance of system functions and manual procedures as part of risk management. Cost is important in these decisions.

4.4.1 PERFORMING THE ANALYSIS

The analysis should assess the net security protection capabilities of alternative sets of countermeasures. This analysis will ensure that appropriate trade-offs between internal and external security protection features are considered. The assessment is largely qualitative, with some degree of subjectivity. It is a way to "force" consideration of alternative countermeasure sets, but should only be used to help make decisions, since the most important attribute of a security protection feature is its effectiveness.

4.4.2 SATISFYiNG SECURITY REQUIREMENTS

The mix of safeguards must meet the minimum security requirements through either automated or manual means, in a cost-effective and integrated manner. Other, less expensive safeguards may be substituted as long as the required level of system security or protection is attained, as determined by the DAA.

4.4.3 RELATION TO SYSTEM LEVEL ANALYSES

DoD Instruction 5000.2 (Part 4) discusses cost and operational effectiveness analysis. Measures of effectiveness gauge the utility of an approach, whereas cost analysis assesses the resource implications. The concept of life-cycle cost is important. Costs of developing, procuring, operating, and supporting system security features must be considered. The cost analysis must include staffing, personnel, and training required in support of the security solution.

4.4.4 EXAMPLES OF TRADEOFFS

Cost-effectiveness comparisons must be made. Choice of security mode involves trading off cost and risk of additional clearances and procedures against the cost and risk of more sophisticated safeguards. Mission performance must also be considered. Reduced automated processing of higher levels or exclusion of users with low clearance levels may impact mission performance. The decision to use a guard to downgrade contaminated data has cost, risk, and performance implications. Options, whereby the computer first supports one level and then is sanitized and supports another level (called periods processing), can also present operational limitations and delay.

4.5 THREAT ASSESSMENT

The intelligence and threat support process driven by DoD Instruction 5000.2 provides procedures keyed to acquisition milestones. Recommended procedures can have significant value in the development of security countermeasures for AISs. When applied to the acquisition of AISs, they permit a logical and orderly look at emerging technical threats, concurrent with the emergence of system definition. This process eliminates the possibility of applying today's (and yesterday's) threat to tomorrow's acquisitions, as is often the case with AIS acquisitions. The System Threat Assessment Report is one successful threat assessment tool promulgated in DoD Instruction 5000.2.

4.5.1 THE SYSTEM THREAT ASSESSMENT REPORT (STAR)

A threat assessment is required for all major programs, and should be initiated for all programs that will process highly classified data or are vital to the Organization's mission. The STAR documents the spectrum of threats against ASs. The intelligence community prepares the STAR and Defense Intelligence Agency (DIA) validates it. For the intelligence community to consider all relevant threats, certain essential documentation needs to be provided, with as much detail as is currently available. Table 4-2 lists the required input to the STAR.

Table 4-2 Input to the System Threat Assessment Report STAR

Functional Description. At an early point in the acquisition process, the Functional Description can be determined from the Statement of Need.

Concept of Operations. Taken from the Mission Need Statement or comparable document, the Concept of Operations provides the overall strategy for using the AIS in an operational environment, and provides information on the equipment, location of deployment, who will operate and maintain the system, and how the system interfaces with other systems.

Data Sensitivity. The most sensitive information that will be processed by the system is identified. If Sensitive Compartmented Information is involved, the supporting Special Security Officer is consulted.

Designated Approving Authority (DAA). Individual(s) who will approve the AIS for operational use are identified. The DAA must consider threats as part of the accreditation decision.

4.5.2 FORWARDING THE INFORMATION

As prescribed by DIA Regulation 55-3, "System Threat Assessment Report," the documentation cited above should be assembled and forwarded through the DAA and command channels to the Special Security Office, which will in turn send it to applicable organizations in the intelligence Community. Emerging ASs often present exploitation opportunities to foreign intelligent services and foreign commercial interests that are not present in weapon systems in the battlefield environment. Unfortunately, the current description of the STAR is keyed to weapon system development and focuses on future battlefield threats. Some slight changes to the DoD 5000.2-M guidance can help to rectify this situation. Suggested changes provided in Table 4-3, specifically addressing emerging AIS's, are taken from an ongoing U.S. Army effort.

Table 4-3 Suggested Changes and Additions to the DoD 5000.2-M

STAR Guidance to Adapt to AISs

Executive Summary and System-Specific Threat - The time frame should start at initial concept definition and proceed through system development, testing, implementation, and the operational lifetime.

Operational Threat Environment - Areas covered should include enemy and friendly adversary operational concepts and activities, organizations, technical equipment, and tactics and techniques which have potential to penetrate, eavesdrop, exploit, or endanger the operating system, application software, and/or databases. These areas should comprise, but not be limited to: potentially harmful activities of friendly adversaries (e.g., computer hackers and disgruntled workers), peacetime belligerent actions, acts of terrorism, low-intensity conflicts, and combat actions in wartime.

Targets - (Recommend deletion for AIS applications.)

System-Specific Threat - Includes:

o Usefulness of data/likelihood if adversary intelligence collection or international technology transfer is directed against the AIS.

o Potential for political events to be shaped or influenced by an adversary to result in a primary or residual effect on the AIS.

- Details of future threats expressed as estimated assessments of employment possibility or probability and the effect these activities would have on the ASS.

- Specific identity and description of threats, as well as capabilities and methods of using described threats.

- In-depth analysis based on doctrine, tactics, techniques, past incidents, capability, as well as probability of occurrence and deployment.

- An integrated assessment should be made of the most probable reactive threat to the AIS.

4.5.3 VALIDATION BY THE DIA

The intelligence community completes analysis, documents the applicable threats, and then forwards the STAR to DIA for validation. The validated STAR will provide a cohesive and integrated threat assessment that addresses all aspects of potential AlS vulnerabilities.

4.5.4 CLANDESTINE VULNERABILITY ANALYSIS

The validated STAR is used for the Clandestine Vulnerability Analysis (CVA) and for risk analysis. NSA recommends a CVA for division/class A1 required systems, but the CVA should also be considered for other ASs that process highly classified information.

4.6 RISK ANALYSIS

From DoD Directive 5200.28," The accreditation of an AIS shall be supported by a risk analysis of the AIS in its operational environment. The risk analysis is an analysis of a System's assets and vulnerabilities to establish an expected loss from certain events." The purpose is to determine if safeguards are adequate to contain potential losses within acceptable limits. Risk is classically determined by summed products of risk to an asset from a threat over some time period (e.g., annually), the value of the asset, the predicted frequency of occurrence of threat, and the percentage of the asset that could be effectively destroyed, compromised, delayed, or denied by the threat.

4.6.1 DIFFICULTIES

Problems arise by a) trying to determine values of non-tangible assets (e.g., classified data), b) trying to determine a reasonable frequency of occurrence from a malicious attacker whose primary weapon is surprise, and c) trying to predict the amount of damage that could actually occur from an attack, which is a function of safeguards, the attacker's capability, the attacker's motive, and chance. (For example, the use of self propagating code usually has unpredictable effects.)

4.6.2 PERFORMING A SUBJECTIVE ANALYSIS

If the DAA cannot locate a suitable risk model, the analysis must deal with the same factors, but in a more subjective fashion. The hacker threat, for example, has predictability in terms of the common viruses. Simple protection approaches are available, but each time a new, more sophisticated threat arises, the defense process begins again. There is no history, and therefore no knowledge, concerning a highly sophisticated attack against DoD command and control installations, but the potential is well understood.

4.6.3 FACTORS IN A RISK ANALYSIS METHODOLOGY

Appendix D of DoD 5200.28-M certain fundamental properties of a risk analysis methodology. They include considering all assets, considering asset losses, identifying vulnerabilities associated with the assets, considering all threats to the system, quantifying risk, and identifying safeguards and protective measures.

4.7 SAFEGUARD SELECTION AND IMPLEMENTATION

Security safeguards are the protective measures and controls obtained to meet the security requirements specified for the AIS. In this guideline, the principal concern is with the COMPUSEC features specified after considering and specifying the non-COMPUSEC safeguards. Acquisition is the vehicle by which the COMPUSEC safeguard selection is accomplished. A contractor is selected from those companies bidding. That contractor proceeds to design, build, integrate, and implement the system.

4.7.1 DEVELOPER RESPONSIBILITIES

The AIS developer is responsible for ensuring the early and continuous involvement of the users, the ISSOs, data owners, and the DAA(s) in defining and implementing security requirements of the AIS. An evaluation plan should be used to show progress toward meeting full compliance with stated security requirements through use of necessary computer security safeguards.

4.7.2 THE DEVELOPMENT ENVIRONMENT

CSC-STD-003-85, known as the Yellow Book, distinguishes between "open" and "closed" secure system development environments. This differentiation depends on a) "whether application developers (including maintainers) have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic," and b) "whether or not configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications." Enclosure 4 of DoD Directive 5200.28 does not use this factor and takes the conservative approach of mandating what was previously the "open environment" table. This is the same as saying that current state-of-the-art configuration control and personnel security procedures are not adequate to protect against the insertion of malicious logic. Nevertheless, configuration control does not erase the need to achieve closed development environments. It points out the importance of decreasing development risk in all ways possible.

4.7.3 REGULATIONS THAT APPLY TO DEVELOPMENT

Enclosure 3 of DoD Directive 5200.28 states a strong minimum security requirement for the developmenb'implementation environment that must be reflected in the acquisition process. Under paragraph 4, Physical Controls: "AIS hardware, software and documentation shall be protected to prevent unauthorized disclosure, destruction, or modification. Unclassified hardware, software, or documentation of an AIS shall be protected if access to such hardware, software, or documentation reveals classified information, or access provides information that may be used to eliminate circumvent, or otherwise render ineffective the security safeguards for classified information. Software development and related activities shall be controlled by physical controls (e.g., two person control) and protected when it is determined that the software shall be used for handling classified or sensitive unclassified data."

4.8 REFERENCES

Several important references address risk management.

a. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)" - This directive defines risk, risk analysis, and risk management. This document also states that the accreditation of an AS must be supported by a risk analysis in its operational environment and that a program should be established for conducting periodic reviews of the safeguards. Finally, in enclosure 4, a risk assessment procedure is provided which is a slight modification to one taken from CSC-STD-003-85, "Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria to Specific Environments."

b. DoD 5200.28-M, (Draft) "Automated Information System Security Manual" - Though still only a draft, this document provides a thorough discussion of the elements of risk management. Appendix D specifically addresses system threat and vulnerability risk analysis.

c. DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria" - A specifiC division/class of this document is selected as a requirement for an automated information system based on the assessed risk index as defined in DOD Directive 5200.28, enclosure 4.

d. FIPS PUB 31, "Guideline for ADP Physical Security and Risk Management" - Addressed are physical destruction or theft, loss or destruction of data and program files, theft of information or other indirect assets, and delay or prevention of computer processing. Topics also include maintenance, reliability, physical protection, and backup.

e. "Information Systems Security Products and Services Catalogue" - This identifies the risk level inherent to evaluated products, based on the level they have achieved in evaluation.

f. CSC-STD-004-85, "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements" - This standard provides guidance for applying the Department of Defense Trusted Computer System Evaluation Criteria to specific environments.

g. NCSC-TG-011, "Trusted Network Interpretation Environments Guideline" - This guideline provides guidance on the use of the TNI in specific environments.

h. DIAR 55-3, "System Threat Assessment Report" (STAR) - This document provides information on threat and threat risk, and is validated by the DIA.

i. DOD Instruction 5215.2, "Computer Security Technical Vulnerability Program (CSTVRP)" - This instruction provides guidance for protection of U.S. technologies.

j. DoD Directive 5220.6, "Industrial Personnel Security Clearance and Review Program" - This directive provides criteria and procedures for determining security clearances of individuals.

k. Gilbert, Irene, "Guide for Selecting Automated Risk Analysis Tools," NlST Special Publication 500-174 - This document presents and evaluates state-of-the-art tools.

l. IMTEC-88-11 and 11S, "Agencies Overlook Security Controls During Development" - This documents the Government Accounting Office Report to Chairman of the Committee on Science, Space and Technology, House of Representatives in 1988.

m. OMB Circular Number A-130, "Management of Federal Information Resources,' Appendix III "Security of Federal Automated Information Systems" - This document requires risk analyses, especially prior to procurement.

n. DoD 5000.2-M, "Defense Acquisition Management Documentation and Reports" - Part 5 of this manual addresses the System Threat Assessment Report and the format.

5 SECURITY TEST AND EVALUATION

5.1 INTRODUCTION

Testing is one of the most important requirements to consider in an AIS acquisition. Testing is the chief way to ensure the security protection features satisfy requirements, whether provided internally or externally. This chapter introduces some of the language and concepts of Security Test and Evaluation (ST&E), an important step in the security risk management process.

5.2 SECURITY TEST AND EVALUATION

5.2.1 TERMS

The terms used in this chapter are defined below. A more detailed discussion of the processes will be given later.

5.2.1.1 EVALUATION

Evaluation is the assessment for conformance with a pre-established metric, criteria, or standard. Security evaluation provides an essential part of the technical evidence required for certification and accreditation. NSA is responsible for evaluating commercial products. Systems are evaluated as part of the certification process. If systems contain NSA-evaluated products, the result of the NSA evaluation can be used as evidence.

5.2.1.2 SECURITY TEST AND EVALUATION

ST&E is a process used to determine if a system's security protection features meet its specification requirements. The process requires documenting and reporting test findings and making recommendations to appropriate authorities based on test results.

5.2.1.3 ENDORSE

To endorse means to sanction or to approve for use. The accreditation process may lead to an endorsement of a system under specific operating conditions and in a specific environment. "Endorsement" does not apply to COMPUSEC products evaluated by the NSA. It only applies to the Endorsed Tools List, used by system developers to identify the formal specification and validation tools that are endorsed by the NSA for use in designing candidate A1 systems.

5.2.2 ST&E AND THE ACQUISITION PROCESS

ST&E begins early in the system life cycle. ST&E includes all the security disciplines (i.e., COMPUSEC, OPSEC, and COMSEC). However, in this guideline, concentration is on COMPUSEC. Before any form of testing can be defined, system requirements must be clearly established. These requirements include the mission the system will perform or support, the associated security requirements, the sensitivity level(s) of information to be processed, user clearance levels, the security mode(s) of operation, and the division/class requirements to be supported. Internal and external controls must complement each other. This process requires an integrated test approach to examine both the elements and the totality of the system's security features. The level of effort required to perform the ST&E is determined by 1) the number of requirements to be proven/satisfied, 2) the difficulty in proving that they are satisfied, and 3) the acceptable level of residual risk determined by the DAA.

5.2.3 USE OF EVALUATED PRODUCTS

A primary goal of NSA is to encourage the widespread availability of trusted systems. This goal is realized, in large measure, through NSA's Trusted Product Evaluation Program. This program focuses on the technical evaluation of the protection capabilities of commercially produced and supported products. Use of systems or system elements evaluated through the NSA program greatly simplifies risk analysis, certification, and accreditation. The level of effort required to perform the ST&E for an acquisition can be minimized through the use of "approved" system products. However, system-level testing will probably not be affected by use of such products. Evaluations can be lengthy, delaying the availability of the product for use in a trusted application. Sometimes, the EPL product version is not the most recent release. These penalties are felt to be small compared to the high assurance and reduction in additional testing.

5.2.4 THE EVALUATION PROCESS

The NSA Trusted Product Evaluation Program focuses on the technical evaluation of the protection capabilities of off-the-shelf systems to meet the COMPUSEC needs of DoD and other Government organizations and agencies. The standards against which products are evaluated are provided by DoD 5200.28-STD, the Trusted Network Interpretation (TNI), the Trusted Database Management System Interpretation (TDI), and the Computer Security Subsystem Interpretation (CSSI).

5.2.4.1 THE EVALUATED PRODUCTS LIST

The product evaluation culminates in the publication of an EPL listing. The evaluation is independent of any consideration of overall system performance, potential applications, or particular processing environment. The EPL is a section in the "Information Systems Security Products and Services Catalogue," prepared by and available from NSA. The aim of the EPL is to provide AIS developers, managers, and users an authoritative evaluation of a product's relative suitability for use in processing sensitive information. The security evaluation of a product is also contained in a formal report available to those requiring more detail.

5.2.4.2 PRODUCT TYPES

Products are separated into general-purpose operating systems, add-on packages, and subsystems. An add-on package runs in conjunction with a specific operating system and is not, by itself, a system that performs all of the functions traditionally ascribed to an operating system. Subsystems are special-purpose products that can be added to existing ASs to increase security and implement only a subset of the security features identified in the procurement criteria. The product evaluation program can be thought of as part of the ST&E to the extent that evidence of evaluations can be used in the ST&E process.

5.2.5 TEST AND EVALUATION (T&E) AND THE LIFE-CYCLE PROCESS

There are three independent types of test and evaluation involving security testing in the life-cycle of an AIS. During Developmental Test and Evaluation (DT&E), technical security measures implemented in the hardware and software are tested to determine the degree of compliance with specifications. Operational Test and Evaluation (OT&E) addresses security from the operational or user viewpoint, and determines the effectiveness and suitability of all security safeguards. ST&E is conducted independent of all other T&E activities. It concentrates on the security features rather than the entire system. ST&E is also performed as part of the risk analysis process to identify threats and vulnerabilities. It uses the risk analysis as input and provides results that are used in further risk analysis. ST&E supports system certification and accreditation decisions. ST&E involvement in the life cycle is as follows:

5.2.5.1 DETERMINATION OF MISSION NEED

Mission analysis and associated threat assessments are factored into the

Program Management Directive and the subsequent Program Management Plan. These documents serve to initiate the ST&E activities during Concept Exploration.

5.2.5.2 CONCEPT EXPLORATION AND DEFINITION

This phase involves a security-focus review of project plans, such as the PMD and PMP, for expected ST&E involvement. Coordination interfaces are established with the Designated Approving Authority, Program Manager, Test Planning Working Group, and Computer Resources Working Group, as well as the DT&E and OT&E organizations. Risk analyses are reviewed and documented in various program documents such as the Test and Evaluation Master Plan. The System Functional Baseline is established upon successful completion of the System Design Review.

5.2.5.3 DEMONSTRATION AND VALIDATION

The feasibility, risks, alternatives, and trade-offs are assessed during the Demonstration and Validation Phase. T&E of computer security features should be conducted for prototype system components. By doing so, technical trade-offs can be used to strike a balance among acceptable risk, mix of authorized user personnel and sensitive data, and the adequacy of security features to meet life-cycle requirements. The overall result of this phase includes a refinement of the requirements and associated T&E plans, objectives, subobjectives, and measures of effectiveness (MOEs). The System Allocated Baseline is established at the end of this phase after the Subsystem Requirements Review.

5.2.5.4 ENGINEERING AND MANUFACTURING DEVELOPMENT

The development phase includes the bulk of DT&E and OT&E activity. Testing individual components, subsystems, and systems is conducted on the actual system as it progresses through preliminary design, detailed design, production, and integration. Formal verification of COMPUSEC features is also accomplished for A1 systems. The impact on performance of embedded computer security features is assessed. The results of these tests become an input to risk analysis and lead to system certification and accreditation. The AIS Product Baseline is established at the end of this phase through the Functional Configuration Audit and Physical Configuration Audit reviews.

5.2.5.5 PRODUCTION AND DEPLOYMENT

Upon receiving a favorable accreditation decision, the system is fielded in the operational environment during this phase. OT&E evaluates the operational system in its operational and support environments. Primary security-relevant OT&E activities inClude evaluating administrative procedures and management functions. Also included are facility planning for physical security, contingencies, and assessment of the AIS's internal and external security features to ensure proper operation. Results are input to the system security certification and accreditation process for Consideration by the DAA for approval to operate the system.

5.3 THE TESTING PROCESS

Responsibilities for ST&E are distributed between the Operational unit and its parent organization/agency. OT&E usually follows DT&E, but in some cases they may overlap or be combined. ST&E is accomplished independently. The following paragraphs summarize DT&E and OT&E highlights. Tables 5-1 and 5-2 show the objectives of DT&E and OT&E, respectively.

Table 5-1 DT&E Objectives

Assess critical issues as specified in program documents

Determine how well contract specifications have been met

Identify and report system deficiencies and vulnerabilities

Determine system compatibility and interoperability with existing and planned equipment or systems

Report reliability and estimate maintainability, availability and logistics supportability

Certify the system is safe and ready for dedicated OT&E

Validate any configuration changes

Assess human factors and identify limiting factors

Assess technical risk and evaluate compliance with specifications

Determine system response or survivability, "hardness"

Verify accuracy and completeness of documents developed to maintain and operate the system

Provide information on environmental issues for impact assessment

Determine system performance limitations

Table 5-2 OT&E Objectives

Evaluate operational effectiveness and system suitability

Answer unresolved critical operational issues

Identify and report operational deficiencies/vulnerabilities

Recommend and evaluate changes in system configuration

Provide information to refine operation and support cost

Determine if documentation and support equipment are adequate

Assess system survivability in the operational environment

5.3.1 DEVELOPMENTAL TEST AND EVALUATION

The implementing command (e.g., the Program Office) must demonstrate that the system engineering, design, and development are complete; the design risks have been minimized; and the system will perform as required in its intended environment. DT&E involves engineering analysis of the system's performance, including its limitations and safe operating parameters. The system design is tested and evaluated against engineering and performance criteria specified to satisfy mission requirements. DT&E also addresses the logistics, engineering, and supportability aspects of the system throughout its life cycle.

5.3.1.1 QUALIFICATION TEST AND EVALUATION (QT&E)

QT&E is normally performed in lieu of DT&E for programs where there is no research and development. These programs might include modifications to existing systems, off-the-shelf equipment requiring minor modifications, and other systems that require no development. Test policies for DT&E apply to QT&E.

5.3.1.2 PREPRODUCTION QUALIFICATION TEST (PPQT)

PPQT is conducted on preproduction hardware and is intended to verify the integrity of the design prior to full-rate production.

5.3.1.3 PRODUCTION QUALIFICATION TEST (PQT)

PQT is conducted on production hardware and is intended to verify the integrity of the manufacturing process.

5.3.2 OPERATIONAL TEST AND EVALUATION

OT&E is conducted under conditions that represent real-life conditions anticipated during the system's life cycle. OT&E evaluates (or refines estimates of) a system's operational effectiveness, maintainability, supportability, and suitability. This process also requires identification of any operational and logistics support deficiencies, and any need for modifications.

5.3.2.1 INITIAL OPERATIONAL TEST AND EVALUATION (IOT&E)

IOT&E usually begins as early as possible in a system's development. IOT&E is structured to provide inputs to the remaining program decisions (e.g., certification). IOT&E is accomplished using prototypes, preproduction devices, or pilot production components. IOT&E must be completed prior to the full-rate production decision to ensure the system is ready for production.

5.3.2.2 QUALIFICATION OPERATIONAL TEST AND EVALUATION (QOT&E)

QOT&E is normally performed instead of IOT&E when there is little or no research and development required.

5.3.2.3 FOLLOW-ON OPERATIONAL TEST AND EVALUATION (FOT&E)

FOT&E is operational testing conducted after the full-rate production decision. FOT&E may also be conducted as needed throughout the remainder of the AIS's life-cycle to assess changes in workload and performance.

5.4 PLANNING AND IMPLEMENTING THE ST&E

Thus far, there has been a discussion of the ST&E in general and its relationship to the rest of the testing process. This portion of the chapter addresses contractual actions necessary to ensure the ST&E is addressed within the overall T&E process. Advance planning, determining what should be tested, determining how testing should be performed, and reporting test results are prime considerations. Although the focus is on contractor actions, the Government is still deeply involved in ST&E. Further, in some instances, the Government may do some of the testing in lieu of tasking a contractor. Regardless, the Government should always review and participate in all aspects of T&E.

5.4.1 TEST AND EVALUATION MASTER PLAN (TEMP)

The TEMP is the primary planning document for T&E. The TEMP is required for all acquisitions. The TEMP should describe the T&E strategy, responsibilities, types of testing, required resources, planned test locations, and milestone schedules. The TEMP is a living document and must be updated as changes occur. From the security standpoint, the ST&E must be explicitly addressed in the TEMP. This is done by tasking the Contractor in the Statement of Work and invoking a CDRL that calls for an a ST&E Annex to the TEMP. A matrix can be used to identify selected security disciplines to be tested.

5.4.2 TEST PLANS

Whereas the TEMP is an overall planning and scheduling document, specific operational test scenarios and events are covered by development and operational test plans. The test plan(s) for ST&E, like other T&E plans, should include test objectives; MOEs; planned operational scenarios; detailed resource requirements; known test limitations; and methods of data gathering, reduction, and analysis. Table 5-3 indicates desired MOE/ MOP(Measure of Performance) characteristics.

Table 5-3 Desired MOE/MOP Characteristics

Sensitivity - Should be sensitive to all potentially significant variables.

Precision - Precise definition is desired to reduce probability of misunderstanding of implications. Penetration testing may be a challenge due to prevalent mindsets. There should be no ambiguities concerning what is being measured and the conditions of measurement.

Feasible Scope - Must not be too broad. For example, a measure for configuration control for a TCB should probably be broken into several measures for change control of DTLS, source code, object code, and implementation documentation.

Independence - Measures should be mutually exclusive to avoid the resultant overweighting of impact(s).

Meaningful - Should be expressed in terms meaningful to the review authority and decision makers (e.g., DAA). This may be a challenge due to technical complexity and or diversity and scope of AIS administration, system administration, or facility provisions.

Measurable - COMPUSEC MOEs/MOPs and their inputs must be measurable to be evaluated. T&E for message or data labeling, for example, may require the capture and recording of data, indicating actual versus correct labeling.

Quantifiable - C0MPUSEC measures should be quantifiable, where possible, to avoid unnecessary subjectivity. However, this does not imply avoidance of critical inputs. Carefully designed questionnaires can gain information from COMPUSEC test personnel on subjects such as resistance to penetration, COMPUSEC performance versus specifications, potential weak links, or areas for effectiveness improvement or cost savings. Also, some otherwise valid measures may not be quantifiable, such as the confidence to be placed in a trusted subject. Analysis may instead be supported by some quantifiable data such as for populations having the same psychological profile and/or clearance level.

Exhaustive - All protective measures in the AIS, administration, and facility must be assessed against variable conditions capable of impacting performance.

5.4.3 TEST REPORTS

The final topic of the test discussion is reporting. Test reports are prepared to document the results of test plan execution. Test reports also identify test objectives, describe the tests conducted, and provide recommendations stemming from test results.

5.5 REFERENCES

a. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)" - This directive establishes the National Security Agency as the evaluator and adviser in the use of trusted computer products and systems. The document also establishes that the individual DoD Components will have responsibility for system test and evaluation.

b. DoD 5200.28-M, (Draft) "Automated Information System Security Manual" - This manual identifies test and evaluation requirements and shows the role of DT&E, OT&E, and ST&E as related to each other as well as to certification and accreditation.

c. DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria" - This standard establishes criteria for evaluating the security features of the component or system.

d. DoD Directive 5215.1, "Computer Security Evaluation Center" - This directive establishes the COMPUSEC evaluation program to be run by NSA for standards, criteria, EPL, and sponsorship of a research and development program.

e. DoD Instruction 5000.2, "Defense Acquisition Management Policies and

Procedures" - Part 8 of this instruction provides policies and procedures for T&E.

f. DoD Directive 5000.2-M, "Defense Acquisition Management Documentation and Reports" - Part 7 of this directive provides the procedures and formats to implement the TEMP.

g. "Information Systems Security Products and Services Catalogue," Prepared by the National Security Agency (Issued Quarterly) - This catalogue provides product evaluation status and results for commercial products evaluated by NSA.

h. NCSC-TG-013, "Rating Maintenance Phase, Program Document" - This document describes a phase of the evaluation program which provides for maintenance of the security ratings across product revisions.

i. NCSC-TG-019, "Trusted Product Evaluation Questionnaire" - This guideline helps builders of systems understand what technical information is required for a product evaluation.

j. DoD-STD-21 67A, "Defense System Software Development" This standard states the requirements for developing, general testing, and evaluating software.

k. DoD-STD-7935A, "Automated Information System (AIS) Documentation Standards" - This standard defines the detailed contents of the Test Plan and Test Analysis Report for general software development.

l. FIPS PUB 48, "Guidelines on Evaluation of Techniques for Automated Personal Identification" - This document provides methods for verifying identity and evaluating the effectiveness of techniques based on a false alarm rate and imposter success rate.

m. NCSC-TG-005, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria" - This document interprets DoD 5200.28-STD in providing criteria for network system evaluation.

n. NCSC-TG-009, "Computer Security Subsystem Interpretation" - This document interprets DoD 5200.28-STD in providing criteria for security subsystem evaluation.

o. NCSC-TG-021 "Trusted Database Management System Interpretation of The Trusted Computer System Evaluation Criteria" - This document interprets 5200.28- STD in providing criteria for DBMS evaluation.

6 CERTIFICATION AND ACCREDITATION

6.1 INTRODUCTION

Chapter 4, "Threat Risk Management - Analysis, Design, and Implementation," discussed the important aspects of conducting a cost/benefit analysis, risk analysis, and safeguard selection for a computer system. Chapter 5 discussed security test and evaluation. These activities in combination, when completed, are the foundation for the next two events in the life cycle of a computer system -- certification and accreditation. For the developer or program manager of a computer system, certification and accreditation are primary objectives, starting at program initiation. This chapter describes the activities involved in achieving these objectives and identifies the documentation required.

6.2 THE CONCEPT

Compliance with the system security policy and development of the risk analysis are critical elements for system certification. The system certification, prepared by the certification authority, is the precursor to system accreditation by the DAA.

6.2.1 TERMS

The following list defines the terms used in this chapter. A discussion of the processes appears later in this chapter.

6.2.1.1 CERTIFICATION

Certification is the technical evaluation of an AIS's security features and other safeguards, made in support of the accreditation process. The technical evaluation establishes the extent to which a particular AIS design and implementation satisfies or complies with specified security requirements. Security requirements are derived from and implemented to negate known, expected, and perceived threats.

6.2.1.2 ACCREDITATION

Accreditation is a formal declaration by the DAA that the AIS is approved to operate in a particular security mode, in a given operational environment, in a specified configuration, and using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

6.2.2 THE PROCESS

Each major activity in the risk management process has several subactivities (which may overlap or be completed out of sequence). Table 6-1 shows this process. Hardware and software provide some, but not all, security protection measures. Other security measures may include physical, administrative, personnel, and procedural steps. Analysis of the system development process (configuration management) and support systems (test tools, training tools, development tools) must be included in the certification and accreditation activities. The hardware and operating system software provide the core of internally enforced security protection features of the system. The computer system application software provides the functionality and implements mission requirements.

Table 6-1 Risk Management Activity

Risk Management Phase	Subactivity

Risk Analysis	Asset Analysis Threat Analysis Vulnerability Analysis
Cost/Benefit Analysis	Economic Assessment
Safeguard Selection and Implementation	Design, Development, and Implementation
Test and Evaluation	Security Test and Evaluation
Certification	Hardware and Basic Software Application Software Operating Site
Accreditation	Computer System (Type) Environment (Site)

6.3 METHODOLOGY

Figure 6-1 shows the certification and accreditation processes. The essence of Certification is a technical evaluation of security protection features against security requirements. In contrast, accreditation is a management decision based on the risk of employing the computer system in an operational environment. Thus, accreditation differs from certification since accreditation is more subjective, while certification is largely objective. Moreover, accreditation decisions require mandatory compliance, whereas certification statements are recommendations to the DAA. A similar methodology can be used for both accreditation and certification, but subtle differences exits. An organized and carefully thought-out methodology will enhance successful certification and accreditation.

6.3.1 TEAM APPROACH

Program Managers assigned to a large program office will have the support of a variety of people. These people will be crucial to technical evaluations or reviews of the contractor's work. A one-person office or small program office will require enlisting the support of other people. Others may include investigative organizations (e.g., security police), personnel administrators, computer systems analysts, and systems programmers. The certification team is usually composed primarily of technical experts. DoD is strongly considering the use of trained certification teams to provide uniform and rigorous certification evaluation, similar to current product evaluation. For accreditation, some technical expertise is necessary, but emphasis will shift to a mission orientation. The DAA will normally be someone from the user organization, but may be higher in the organization, or the owner of the protected data. Therefore, the functional user and the implementing organization must be well represented.

6.3.2 GOVERNMENT OR CONTRACTOR PERSONNEL

The Government often has insufficient resources to perform certifications and therefore, supplements its staff with contractor personnel. Each program will use a different mix of personnel, but the resulting package of documents will be substantially the same, independent of the mix. This mix makes planning and coordination one of the most important functions.

6.3.3 ITERATIVE PROCESS

The entire process (certification or accreditation) is iterative since, based on the findings from each step, previous steps may need to be re-examined. Moreover, some aspects of each step may need to proceed at the same time, perhaps by different evaluators. Again, the role of coordinator becomes very important. In accreditation, because the final decision can be postponed (e.g., interim versus final), the process could continue for much longer than scheduled.

6.3.4 STRATEGY

The basic strategy should be to develop a comprehensive plan, get all the players to agree (most importantly the DAA), and then execute the plan. When completed, the result will be a package to be taken to the certifying official or DAA for review and approval.

6.4 CERTIFICATION

The certification process ideally begins when the computer system acquisition is conceived, and continues throughout the system's life-cycle. Certification occurs when the certifying official Signs a letter stating the system security protection features have been evaluated and found to be adequate and correct. The letter signed by the certifying official typically has a number of attachments, including risk analyses, test reports, security features, residual risks, cost/benefit analysis, and others. Completion and compilation of the attachments in the certification package involve the Program Manager. The certification team leader should carefully determine the number, scope, and applicability of the documents to meet the certification requirements.

6.4.1 KEY ELEMENTS

The Certification Package has two key elements: analysis of the security features and the supporting documentation.

6.4.1.1 ANALYSIS OF SECURITY FEATURES

The technical analysis of the security features is the basis for certification. A report documents the results of the analysis, with the following objectives:

a. To document the adequacy and correctness of the security protection features in satisfying security requirements. This process involves comparing the "build to" (design) configuration to the "as built" (installed or implemented) configuration.

b. To assess supporting documentation completeness, accuracy, and consistency.

c. To identify latent system security vulnerabilities discovered in this evaluation. Countermeasure(s) will be recommended and the acceptability of the associated risk(s) will be assessed if countermeasures are not applied.

d. To reveal limitations or restrictions necessary for the computer system to meet acceptable risk when the system is fielded and functioning in the selected security mode of operation.

e. To present recommendation(s) based on conclusion(s) derived from the evaluation.

6.4.1.2 SUPPORTING DOCUMENTATION

The Certification Package, whether prepared by the Government or the contractor, must contain a set of supporting documents. These documents are necessary since they "prove," or provide tangible evidence, that necessary actions have been completed. The certification team leader should carefully determine the number, scope, and applicability of the documents to match the certification requirements. Only necessary documents that address residual risk will be required for each computer system to be accredited. A statement should be included in the certification letter identifying the supporting documentation being provided. It is recommended that a minimum set of attachments accompany the certification letter submitted to the DAA. The certification package should contain documentation that will not only assist in the DAA making the decision to operate, but also assist any future recertification and reaccreditation of this system or a similar system. Table 6–2 identifies the supporting documents.

Table 6–2 Supporting Documentation

Certification Letter (signed by the certifying authority)

Risk Assessment and Risk Analysis

Cost/Benefit Analysis

Development Test & Evaluation Test Reports (or security– relevant extract if security testing was incorporated in other tests and not done separately)

Operational Test & Evaluation Test Reports (or security–relevant extract if security testing was incorporated in other tests and not done separately)

Clandestine Vulnerability Analysis (unclassified synopsis)

Certification Statement (from the Personnel Clearance Authority)

Certification Statement from security investigative organization (for resource protection)

Evaluated Products List (or extract)

Waivers, Pending or Approved (Waivers should always be subject to periodic review, at least every six months. The risks to be accepted by virtue of the waiver should be clearly identified.)

Other Pertinent Documents (e.g., Independent Verification and Validation Reports)

Mission description, system configuration, residual risks, list of other interconnected systems security features, and any previous certification/ accreditation

6.4.1.3 SUPPLEMENTARY DOCUMENTATION

Several other documents are not technically part of the Certification Support package; however, they are necessary for background material (e.g., test plans), to demonstrate the computer system is ready for the field (e.g., Trusted Facility Manual), or to prepare for the next phase, accreditation. Not every document will be required for each computer system program. In that case, a statement should be included attesting to a document's non-applicability. Table 6-3 lists the supplementary documents.

6.4.2 GOVERNMENT-CONDUCTED CERTIFICATION ACTIVITIES

For a program in which the Government will be doing the bulk of the certification effort, the certification process is typically done in four steps:

Table 6-3 Supplementary Documentation

Trusted Facility Manual (TFM)

Security Features User's Guide

Developmental Test & Evaluation Test Plans (or security- relevant extract)

Operational Test & Evaluation Test Plans (or Security-relevant extract)

System Security Plan

System Security Concept of Operations

Security AIS Requirements (from the Contract)

Executive Summary from the Descriptive Top-Level Specification

Trusted Computing Base Verification Report (unclassified synopsis for Class A1)

Covert Channel Analysis Report (unclassified synopsis)

Installation Procedures for Security-relevant hardware and software

Maintenance Procedures for Security-relevant hardware and software (if not in the Trusted Facility Manual)

List of the members of the Certification Support Analysis Team (with a brief resume of their technical qualifications)

Other Pertinent Documents (e.g., contingency plans not in the Trusted Facility Manual and special procedures for cryptosecurity systems)

Configuration Management Plan, Evaluated Products Final Evaluation Report (unclassified), Security Classification Guide, Site Surveys, other agencies/ individuals not directly part of the C&A team, and rationale for tailoring the effort.

6.4.2.1 PLANNING

Planning tasks include:

6.4.2.1.1 HIGH-LEVEL REVIEWS

The plans should require certification analysts to perform high-level reviews of the entire system or application to gain an understanding of the security-relevant issues involved. The plan should also define problem areas and anticipate the need for specialized skills.

6.4.2.1.2 PLACING BOUNDARIES ON THE EFFORT

During the planning phase, boundaries must be defined for all facets of the system and application environment. This includes the administrative, physical, and technical areas. Without this comprehensive review and bounding, the results might give an incomplete, and perhaps misleading, picture of the security posture of the system or application.

6.4.2.1.3 PARTITIONING THE WORK AMONG AVAILABLE ANALYSTS

A certification project is usually partitioned based on the analysts' specialized skills.

6.4.2.1.4 SCHEDULING AND PLANNING

Scheduling of tasking must be established so as to ensure availability of personnel, facilities, and necessary resources. Careful planning will reduce scheduling conflicts and delays in accomplishing testing.

6.4.2.1.5 IDENTIFYING AREAS TO EMPHASIZE

The planning emphasis should be directed to areas having a greater potential for loss of, or risk to, sensitive information. These areas may have been identified in an earlier risk analysis, problems identified during testing, or in reports of past problems with similar systems.

6.4.2.1.6 SKETCHING OUT THE DOCUMENTATION REQUIREMENTS

The data collected during the planning phase forms the basis for meeting the documentation requirements of the certification process. Specific attention should be paid to security requirements, evaluation approach, evaluation team composition, tasks and schedule, required support, and certification products and reports.

6.4.2.1.7 ASSUMPTIONS AND CONSTRAINTS

The quality and availability of the required documentation, access to or availability of the system for the C&A team, the Program Manager's schedule, and training of C&A team members, should be addressed.

6.4.2.2 DATA COLLECTION

The ideal source of information is existing system documentation. However, there are occasions when the necessary documentation does not exist or is not in a form to be readily analyzed. An efficient technique for gathering information is for application personnel to provide briefings to the certification team. Document reviews and interviews are also often needed to expand upon and corroborate the information found during the evaluation. Critically needed documents deal with issues in Table 6-4.

Table 6-4 Data Collection Sources

System application or security requirements

Risk analyses portraying threats

Block diagrams showing inputs, processing steps, and outputs, along with complete transaction flows for important transaction types

System personnel desktop procedures for the system

Functional descriptions of security controls or protection features

Accreditation package(s) from external systems to include residual risks

6.4.2.3 CERTIFICATION EVALUATION

Four major tasks comprise a basic certification evaluation, they are as follows:

6.4.2.3.1 SECURITY REQUIREMENTS EVALUATION

A security requirements evaluation is important because certification is more accurate if the application or system has well-defined security requirements. This task critiCally examines the security measures documentation for compliance with National, DoD, and user security policy and protection safeguard requirements. Four primary areas must be considered when defining system or application safeguards: assets, exposure potentials, threats, and controls. The risk analysis may define many of the security safeguards. Other useful evaluation tools include computer security checklists and questionnaires.

6.4.2.3.2 SECURITY PROTECTION FEATURE EVALUATION

A security protection feature evaluation determines whether security features or functions such as access authorizations, operational usage monitoring, password generation and management, and sensitivity indication labeling, satisfy all current security requirements. Ill-defined requirements cause this part of the overall evaluation to become the most important task in the basic evaluation. The primary evaluation method is use of a checklist based on the stated requirements. Detail should be given to the functional specification level.

6.4.2.3.3 SECURITY CONTROL IMPLEMENTATION

Security functions described in the documentation must be properly implemented. The existence of physical and administrative controls can be confirmed by inspection, but assurance for internal controls requires testing. In some cases, a brief demonstration may be all that is required; in other instances, elaborate tests must be devised, validated, and conducted to gain the necessary assurances.

6.4.2.3.4 METHODOLOGY REVIEW

One way to determine whether security controls have been properly implemented is to examine the methodology used to design and develop the system or application. Several areas of concern exist when reviewing a system or an application development methodology for certification: documentation, objectives, project control, tools and techniques, and resources.

6.4.2.4 REPORT OF FINDINGS

The Report of Findings is the primary outcome of the certification process. The certification official has the Opportunity, not only to report evaluation results to the DAA, but to explain the potential ramifications of the findings in terms of risk to the system. Recommendations can be made to correct deficiencies temporarily or permanently and identify the potential security risk ramifications. Based on the recommendations of FIPS PUB 102, another recommendation can be to conduct a more detailed certification evaluation in particular areas, where the certifying official feels that the current evaluation was inadequate.

6.4.2.5 CLASSIFICATION OF FINDINGS

The disclosure of information which, if exploited, could impact the mission of a system or allow security features to be bypassed, must be protected from disclosure to unauthorized persons.

6.5 ACCREDITATION

Accreditation is based on the premise that a single individual, the DAA, is the accreditor. He/she exercises management's prerogative to grant (or deny) authority for a computer system to process actual mission data in an operational environment.

6.5.1 CONSIDERATIONS

In making the accreditation decision, the DAA considers a number of factors:

6.5.1.1 THE MISSION

The DAA's first concern is for operational mission requirements to be met.

6.5.1.2 THE THREAT

There will always be threats to sensitive information. The threats, coupled with the system's vulnerabilities, provide the risks upon which to focus the security protection features.

6.5.1.3 THE COUNTERMEASURES

Adequacy of the security protection features in countering identified threat vulnerability pairs will be determined.

6.5.1.4 THE RISK

Residual risks will be assumed by the DAA if the computer system is approved for operation.

6.5.1.5 THE COST

The costs to reduce residual risk could be in terms of dollars, schedule, performance, or other resources.

6.5.2 KEY ELEMENTS

Like certification, the two key elements to the accreditation decision package are assessment of risk and the supporting documentation.

6.5.2.1 ASSESSMENT OF RISK

The subjective assessment of risks associated with employing the AIS is the basis for accreditation. The results of the assessment are documented in a report with the following objectives:

a. To assess the security risks associated with employing the AIS. This assessment should include normal operations, degraded mode operations, and stressed operations.

b. To evaluate the supporting documentation in terms of completeness, accuracy, and consistency.

c. To identify and evaluate any latent system security vulnerabilities discovered and recommend countermeasures, or assess the acceptability of the associated risks.

d. Identify any limitations or restrictions necessary for acceptable risk when the computer system is fielded and functioning in the selected security mode of operation. Identify the basis for provisional or interim accreditation, if applicable.

e. Document any action items necessary to achieve a favorable accreditation decision.

f. Provide conclusions and recommendations based on this assessment.

6.5.2.2 SUPPORTING DOCUMENTATION

The Accreditation Package, whether prepared by the Government or the contractor, must contain a set of supporting documents. Table 6-5 lists this documentation.

Table 6-5 Accreditation Supporting Documentation

Mission impact statement attesting to the urgency and criticality of the computer system from the operational user or functional area supported

Recommended Accreditation Letter

Certification Package for the computer system, with supporting documentation (required for both Type and Site Accreditation)

Certification Package(s) from the Computer System Facility Manager(s), with supporting documentation (required for Site Accreditation)

Waivers, pending or approved

Action Items

Security Features User's Guide

Trusted Facility Manual (TFM)

Clandestine Vulnerability Analysis (unclassified synopsis)

Installation Procedures for security-relevant hardware and software

Maintenance Procedures for security-relevant hardware and software (if not in the TFM)

Other Pertinent Documents (e.g., contingency plans not in the TFM, special procedures for cryptosecurity systems)

6.5.3 CONTRACTOR-PROVIDED ACCREDITATION SUPPORT

For an acquisition in which a contractor will provide the accreditation package, the approach is nearly the same as for certification. The contractor needs to be given contacts and documents on the accreditation requirements and his role.

6.5.3.1 STATEMENT OF WORK TASKS

Include two Statement of Work tasks in the RFP:

6.5.3.1.1 ACCREDITATION PLAN

Require the contractor to deliver to the Government a plan documenting the actions necessary to achieve computer system accreditation.

6.5.3.1.2 ACCREDITATION SUPPORT

Require the contractor to execute the Accreditation Plan, and deliver an Accreditation Support Package to the Government.

6.5.3.2 GOVERNMENT REVIEW

Again, review the contractor's submissions for completeness, accuracy, and reasonableness. Comments provided back to the contractor must be ensured to represent a coordinated Government position.

6.5.3.2.1 ACCREDITATION PLAN

Ensure the planned actions "track" with the system security specifications and the computer system program operational environment. Planned actions must be coordinated with a variety of offices so there are no surprises later as the plan is executed.

6.5.3.2.2 ACCREDITATION SUPPORT

Ensure the documents in the Accreditation Support Package are current, complete, and accurate. This process will require a careful review by both technical and functional area experts in various disciplines.

6.5.3.3 BRIEFING

The DAA will probably expect to be given a briefing before making a decision. Whether this briefing is prepared by the contractor or internally, the content of the Accreditation Support Package should provide the information.

6.5.4 GOVERNMENT-CONDUCTED ACCREDITATION ACTIVITIES

In a program in which the Government will be doing the bulk of the accreditation effort, follow the same approach outlined for a contractor.

6.5.5 MANAGING PROBLEMS

Since systems or applications requiring certification and accreditation are usually vital to an organization's mission, some problems discovered may not be severe enough to remove or delay the system or application from operational use. If the problems are major, alternatives are available for authorizing operational use. The choice of alternatives depends on the nature of the problem and the operational mission.

6.5.5.1 THE DECISION

The following accreditation decisions could be made:

6.5.5.1.1 GRANT FULL OPERATIONAL AUTHORITY

In this case, no restrictions apply.

6.5.5.1.2 GRANT CONDITIONAL OPERATIONAL AUTHORITY

Here, permission to Operate might be for a temporary time period, or require additional security protection features (e.g., until security feature "X,' is corrected, tested, and certified, no information more sensitive than "Y" can be processed).

6.5.5.1.3 GRANT LIMITED OPERATIONAL AUTHORITY

In some instances, authority to operate might be restricted to a specific operational circumstance or mode (e.g., only during crisis, or only in the Dedicated Security Mode).

6.5.5.2 CAVEATS

When systems must be operated with major problems, conditional or limited authority may be granted. This is an interim measure only, pending implementation of additional security features. A review schedule and continuing oversight is necessary to ensure conditions of the interim accreditation are adhered to, and additional security features to be implemented are not forgotten.

6.5.5.3 PROVIDING ADDITIONAL SECURITY PROTECTION FEATURES

Several areas should be considered if the AlS requires additional security protection.

6.5.5.3.1 ADDING CONTROLS

Security protection controls may be added, but they will usually be limited to procedural or physical measures. It is not usually practical or cost-effective to add internal controls late in the program.

6.5.5.3.2 RESTRICTING PROCESSING

Processing could be restricted to non-sensitive information only, or to a lower level of sensitive information than planned. Or, the security mode of operations could be changed to provide a higher level of confidence or protection.

6.5.5.3.3 REMOVING VULNERABLE FUNCTIONS

Selected functions causing major problems or creating high risk could be removed or their implementation delayed.

6.5.5.3.4 RESTRICTING USERS

The number of users, or their privileges, could be restricted.

6.5.5.3.5 REMOVING REMOTE ACCESS

Remote terminals could be physically or logically disconnected when sensitive information is stored or processed.

6.6 HANDLING RESTRICTIONS AND SENSITIVITY MARKINGS

Both the Certification and Accreditation Packages must be marked, handled, and controlled consistent with the classification of the information they contain. When possible, classified information should be placed in a separate appendix to the packages; in any event, classification markings are required in accordance with DoD Directive 5200.1-R.

6.7 REFERENCES

The most important references for certification and accreditation are:

a. DoD Directive 5200.28, "Security Requirements for Automated Information Systems" - This directive requires assurance that adequate security measures have been taken for operational system use and that an accreditation must be accomplished and approved by the DAA.

b. DoD 5200.28-M, (Draft) "Automated Information System Security Manual" - Section 4 of this document deals with certification and accreditation, along with testing. This document identifies the relationships between product evaluation and certification.

c. FIPS PUB 102, "Guidelines for Computer Security Certification and Accreditation," U.S. Department of Commerce, NBS - This guideline contains detailed discussion on the management of certification and accreditation, roles, application certification plan, security evaluation report, and recertification and reaccreditation.

d. "Information Systems Security Products and Services Catalogue" - This catalogue is prepared by the National Security Agency and issued quarterly. The document provides reports on the evaluated products critical to certification of a system.

e. DoD 5200.28-STD, "DoD Trusted System Evaluation Criteria" - This document describes protection mechanisms and provides assurance requirements to be met as a condition for certification.

f. NCSC-TG-01 5, "A Guide to Understanding Trusted Facility Management" - This guideline discusses the support of security and accountability policies throughout a system's operation via the separation of functions between administrator and operator and between security-relevant and non-security-relevant functions of the system administrator.

g. NCSC-TG-026, "A Guide to Writing the Security Features User's Guide for Trusted Systems" - This guide discusses the motivation and meaning behind the DoD 5200.28-STD requirement for a Security Feature User's Guide.

h. NCSC-TG-028, "Assessing Controlled Access Protection" - This guide is intended to be used by individuals tasked to perform a technical analysis of an AIS in support of its certification and accreditation.

i. DoD Directive 5200.1-R, "Information Security Program Regulation" - This regulation provides guidance to help determine the security level in the completed accreditation package.

j. NCSC publications under development:

(1) "Introduction to C&A Concepts" - Provides a baseline description of the current state of C&A. C&A terms are standardized; a high-level description of the standard C&A process is included; and some of the key issues are discussed. This document is viewed as introductory and envisioned to have a limited life-span. (Second draft is out for review; expected publication date is January 1993.)

(2) "The Certification Process Handbook" - Outlines high-level generic C&A process in more detail as well as some tailoring guidance for specific applications or environments. More comprehensive tailoring guidance will be promulgated later as more specific methodologies are developed. (First draft due by July 1993; expected publication date is December 1993.)

(3) "DAA Guide" - Executive level document that describes the C&A process, provides the accreditor with descriptions of responsibilities as well as sources for information, and gives an overview of what the DAA should expect from the certification process. (First draft due by July 1993; expected publication date is December 1993.)

(4) "Guidance for Developing a C&A Plan" - Addresses developing a C&A plan for systems that already exist as well as for new acquisitions. Provides a Program Manager with some guidance as to the level of effort required for certification and accreditation. (First draft due by July 1993; expected publication date is December 1993.)

7 MANAGING THE ACQUISITION OF SECURE SYTEMS

7.1 INTRODUCTION

At this point of the document, it becomes apparent that many program tasks are performed by people other than the Program Manager. Since there is a security "thread" running through all portions of the program, other activities may either directly or indirectly affect the security arena. Chapter 2, The Acquisition Process, provided an overview of four separate, but interrelated "chains of management" associated with an acquisition. This chapter will focus on the Program Management chain, its associated elements and documents, and its application to secure systems. It will show how those responsible for security will support Program Management in this acquisition. This chapter also covers the basic life-cycle phases of a project, and identifies the security-relevant data deliverables. Appendix B summarizes plans and deliverable documents.

7.2 MANAGEMENT POLICY AND OBJECTIVES

DoD Directive 7920.1, Life-Cycle Management of Automated Information Systems, contains the DoD automated information system management policies and objectives. Policies and objectives should be considered while addressing security for any automated information system acquisition.

7.2.1 POLICY

The key management policy regarding security states that the design, development, acquisition, operation, and management of an automated information system must meet security policy directives and regulations, while at the same time meeting mission requirements.

7.2.2 OBJECTIVES

The Program Manager's role is a direct result of the DoD's concern for security. The Program Manager is the person who must ensure security protection requirements are satisfied during an automated information system acquisition.

7.2.3 THE FUTURE

In the future, functional users will increasingly state their requirements for "trusted" automated information systems. In response, the DoD will have to be part of the "leading-edge" of technology as it strives to meet both functional user operational requirements and mandates for security. It is important for the Program Manager to get to know the user early.

7.2.4 USER EDUCATION

A major procurement responsibility is to educate functional users so they understand how both their operational and security requirements will be met. This can be accomplished through user awareness and training.

7.3 PROGRAM MANAGEMENT ACTIVITIES

7.3.1 PLANNING

Automated information system planning is like all other planning activities. Planning is required to meet policies and objectives and is the first step necessary to compete for and to get approved resources. The planning process must be kept in mind for several reasons:

7.3.1.1 HOW THE PROGRAM MADE IT THIS FAR

Proper planning (or the lack thereof) has evolved the automated information system program to its current point in time.

7.3.1.2 INADEQUATE RESOURCES

Competing for funds and resolving "disconnects" is difficult. Resources necessary to satisfy the security issues not properly addressed at program inception are likely to cause iteration of the planning phase and could even result in serious delays.

7.3.1.3 HEADS-UP

The long range planning documents help all planners understand future requirements. Proper inputs during the cyclical document updates will ensure the program gets the resources and solutions for security requirements it needs.

7.3.2 MANAGEMENT

Program management is a necessary ingredient for any acquisition. There are two primary objectives:

7.3.2.1 CONTROL MECHANISM

First, program management establishes controls to ensure automated information system operational requirements are developed on time and within budget. These controls are provided through a system of checks and balances. Since the approach for "trusted" systems is a recent technology, it may involve acquiring a unique or "tailored" product (this usually translates into a more "costly" product). Until the technology matures, the level of effort required to bring a "trusted" system into the organizational inventory will be considerable, dictating sound program management tools and controls.

7.3.2.2 LIFE-CYCLE SUPPORT

The second program management objective is to ensure program support throughout the life-Cycle. This may entail millions of dollars and hundreds of people.

7.3.3 COMMUNICATION

The program manager must recognize that the key to a successful program is early and continuing communication among security people, and between security and systems people. The primary elements affected by program management are systems engineering, configuration management, and test and evaluation management. Since a major impetus behind a "trusted" automated information system acquisition is security, the Program Manager will be heavily involved in all three of these program management elements.

7.3.3.1 SECURITY MANAGEMENT

DoD Instruction 5000.2, Part 5F deals with security during development. Part 6J addresses security in the design. The Program Manager can expect to be tasked to work many of these items or processes. He/she should review this document keeping the security "thread" in mind. The Program Manager may be the Security Manager or another person appointed to fill the slot. The rest of this chapter will refer to the Security Manager when security management activities are discussed.

7.3.3.2 TECHNICAL REPRESENTATIVE FOR CONTRACTS

The contracting officer is not usually technically qualified in the intricacies of security in an automated information system acquisition. Therefore, the Security Manager may expect to be tasked as a Contracting Officer Technical Representative (COTR) on security-relevant issues.

7.3.4 COORDINATION

There will be extensive coordination with other agencies for both the program manager and the security manager.

7.3.4.1 STANDARD AUTOMATED INFORMATION SYSTEM ASSETS

Certain systems have been designated as "standard" automated information systems. These standard systems are generally defined as automated information systems serving more than one organization. These systems must be coordinated at a higher command level or with an organization specifically tasked for their management. Coordination with other organizations will be required if the program interfaces with one or more of these standard systems.

7.3.4.1.1 LEAD-TIMES

Some of the lead-times for specific standard systems can be quite lengthy. As a minimum, the Program Manager should check for any requirements to link with or use AUTODIN, military service telecommunications systems, DDN, DCS, leased long-haul services, MILSATCOM, and WWMCCS. Not only must the specific program's security requirements be met, but also the interface security requirements of the standard system programs. That is, program security requirements may have to be engineered and "dove-tailed" to access or emulate connections already on these systems and accreditation must be accomplished by these systems. Ideally, interface security issues should be considered during the conceptual phase when the interfacing framework and flows are first being addressed. Delaying addressing interface security issues means major revisions will almost certainly be required as the program matures.

7.3.4.1.2 INCREASE IN TRUSTED SYSTEMS

As "trusted" systems become more prevalent, they will increasingly impact on and interface with those automated information systems already designated as standard systems. Though the evolution of "trusted" systems is not yet near this point, there may come a time when one or more trusted systems are designated as standard Systems.

7.3.4.2 COORDINATION WITH NSA

Some programs are the sole responsibility of the operational organization. However, other programs may need assistance from the National Security Agency (NSA). This agency provides policy guidance and technical support to DoD organizations for automated information system security activities. This includes evaluating specifications, statements of work, and test plans. Sufficient lead time must be allowed to program necessary resources.

7.4 PREPARING THE PROGRAM PLAN

7.4.1 ISSUES PRIOR TO PLAN PREPARATION

The Program Management Directive (PMD) provides direction to participating commands and authorizes the program to proceed. The PMD gives a broad allocation of resources and levies major tasks on the players. The PMD serves as the source document for developing all further documentation. Although developing and maintaining the Program Plan is primarily the responsibility of the Program Manager (PM), the Security Manager is in the best position to give advice on security matters. The following three major factors must be addressed:

7.4.1.1 LOW COST

The Program Manager is responsible for complying with the Federal Acquisition Regulation (FAR) and DoD Directive 7920.1, Life-Cycle Management of Automated Information Systems, ensuring the automated information system is developed, acquired, evaluated, and logistically supported at a low cost. To do this he/she must comply with several requirements.

7.4.1.1.1 HARDWARE REUSE

DoD Directive 7920.1 Life-Cycle Management of Automated Information Systems requires automated information systems to be acquired from commercial sources only if the requirement can not be met through the DoD reutilization program. This guidance must be followed, but the chance of a suitable, reused "trusted" system is very low, This is true for two reasons. At present there are only a handful of trusted systems in existence. Until the "trusted" technology has had time to mature, excess" trusted equipment will not be available. Secondly, equipment appearing on the Evaluated Products List (EPL) has been fielded; however, the equipment could be at the end of its economic life, making reuse unreasonable.

7.4.1.1.2 SOFTWARE REUSE

Besides the hardware reuse requirement, the Program Manager must also comply with the Federal Software Exchange Program by not procuring duplicate software. The comments regarding equipment also apply to software. At this time most "trusted" software is machine specific and "tailored" for each application. A major objective of the Information Systems Security Products and Services is to encourage private industry to develop "trusted technology."

7.4.1.1.3 OTHER SOURCES

The PM must also consider "other sources" to realize a low cost. Although there is a slim chance of "piggybacking" on a "requirements contract" for the trusted System, it is unlikely one will be found which meets your requirements. One of the tasks is helping others realize these kinds of procurements will be unique until Government and industry have considerably more experience in this arena. "Business as usual" can not be expected.

7.4.1.2 PROGRAM FUNDING PROFILE

The PM is responsible for determining the specific resources required to implement the program and the funds needed to acquire the system. It must be ensured that security-relevant resources are priced and included in the profile. While some historical data is available, precisely allocating costs between external and internal security measures for a "trusted" system may be difficult. Early in the program when requirements are still being gathered or defined, a good "rule of thumb" is to use the cost for a System High Security Mode. This would provide costs for a complete suite of external controls and create a fiscal planning "hedge" for internal controls. As security requirements become better defined, the program security costs can be more precisely determined.

7.4.1.3 PROGRAM STATUS REPORTING

Although a Program Manager responsibility, status reporting is of vital interest. The Security Manager should arrange with the PM to have documents impacting security (e.g., Engineering Change Proposals) coordinated and provided from program inception. Changes should also be coordinated. Since the Program Manager has to specify reporting procedures in the Program Management Plan, information requirements should be identified early. Doing so will make tracking security-relevant issues easier, rather than attempting to "capture" the data later. It is also important to compile complete data to facilitate the elaborate documentation required for the certification and accreditation processes.

7.4.2 PROGRAM MANAGEMENT PLAN

This is the master plan for the automated information system acquisition. There are two primary interests in the writing of the Program Management Plan.

7.4.2.1 PROGRAM MANAGEMENT STRUCTURE

The first interest is the section describing the program management structure and the relationships between the functional areas. The Program Management Plan should delegate to the Security Manager the authority to work security issues. The Program Management Plan should also clearly state the precedence security issues have in the scope of the program. An adequate structure should provide for consultation and coordination during each step in program development. If the Security Manager has been brought into the picture after the initial Program Management Plan has been released, and its organizational structure and relationships do not adequately address security, there must be a renegotiation of this portion of the Program Management Plan with the PM as soon as possible.

7.4.2.2 "CALL-OUT" OF SUPPORT PLANS

The second interest is the section devoted to "calling-out" support plans. For a major automated information system acquisition, a complete suite of support plans is warranted because there are so many different security facets to consider. More detail on the various support plans can be found below.

7.5 CONCEPT DEVELOPMENT

The Mission Need Statement (MNS) has a logical course and required elements. One required element in the MNS format is the Concept of Operations (CONOP). A Concept of Engineering (COE) and a Concept of Maintenance (COM) may also be presented in the MNS. However, if the last two concept statements are not in the MNS, they will usually be developed by the Program Management Office (PMO). The Security Manager should expect to help write and evaluate all three of these documents.

7.5.1 CONCEPT OF OPERATIONS

Prepared by the functional user, the CONOP is a description of the environment and intended use of the automated information system. The CONOP has a security section that gives broad security guidance for the program. This section should include the sensitivity assessment, security mode of operation, and both hardware and software security mechanisms. Major programs generally have a separate System Security Concept of Operations (see Chapter 4, Threat Risk Management).

7.5.2 CONCEPT OF ENGINEERING

The COE is a description of the overall approach to system engineering, usually prepared by the PMO. The COE addresses the equipment and software necessary to meet the needs of the user. The COE should use DoD 50t0.12-L terms to portray the engineering definition of the complete system. System engineering is required for a trusted system. The Concept of Engineering should address configuration management, software development, quality assurance, technical performance measurement, test and evaluation, and risk management.

7.5.3 CONCEPT OF MAINTENANCE

The COM is a description of the overall approach to maintaining the automated information system. The COM is usually prepared by the Program Management Office and must satisfy DoD Instruction 5000.2 (Part 6C) reliability and maintainability requirements, to satisfy the operational objectives specified in the CONOP, COE, and PMD. In a broad-brush manner, the COM discusses reliability, maintainability, sustainability, maintenance requirements, and performance criteria.

7.5.4 CONCEPT AND SUPPORT PLANS

Support plans discussed below, and their related concepts, are provided in Appendix B.

7.6 SUPPORT PLANS

Each of the three functional concept descriptions (CONOP, COE, and COM) may be logically "linked" with specific support plans "called-out" by the Program Management Plan. These support plans have the details for the security "thread." Inputs and coordination should be provided on each of them.

7.6.1 SUPPORT PLANS RELATED TO THE CONCEPT OF OPERATIONS

There are two support plans related to the Concept of Operations.

7.6.1.1 SURVIVABILITY SUPPORT PLAN

This plan describes the ability to survive, reconstitute, and sustain operations. The plan should require "recovery" capabilities to obtain and transport duplicates of operating system and applications software and data files. Redundancy, alternate sites, and off-site arrangements are often key elements for survivability.

7.6.1.2 TRAINING SUPPORT PLAN

The Training Support Plan should include training in the security disciplines for both operations and maintenance personnel. This plan should include a module on system Security and provide the system administrator, security officer, maintainers, and users specific training commensurate with their level of system involvement. Security training is a necessary ingredient of computer security, whether for Government or contractor personnel. There are three cases to consider: a) contractor personnel may attend a contractor "in-house" training course, b) Government personnel may attend a contractor course, or c) Government personnel may attend a Government course. Each case should provide a measure of assurance that security training is properly weighted in the course program. Early planning is a necessity because the lead time to respond to a new requirement is significant.

7.6.2 SUPPORT PLANS RELATED TO THE CONCEPT OF ENGINEERING

Here, seven support plans have been identified as relating to the Concept of Engineering.

7.6.2.1 CONTRACTING AND ACQUISITION SUPPORT PLAN

This support plan should indicate the Security Manager's participation in the Data Call and the Data Requirements Review Board. This plan should acknowledge that security is a driving cost factor in the acquisition. The plan may also specify that the Security Manager serve as the Contracting Officer Technical Representative on all security issues. The Plan should reserve a place in the preparation of the Request for Proposal (RFP) and Statement of Work (SOW) for security requirements and specifications. See MlL-HDBK-245B and the Federal Acquisition Regulation (FAR) for details on the content and structure of the RFP. See volume 2 of this guideline series for details on the content and structure of a SOW.

7.6.2.2 SOURCE SELECTION PLAN

The Source Selection Plan was addressed in Chapter 2, section 2.5.2.4, and will be further addressed in the fourth document of this guideline series. This plan describes the organization, roles, responsibilities, and functions of the Source Selection Evaluation Board (SSEB). This plan outlines award criteria and "evaluation factors" along with the scoring methodology. The Security Manager should prepare the security-relevant portion of the plan and participate in SSEB activities. He/she should expect to chair the Security Panel of the Technical Team. The very important Proposal Evaluation Guide (PEG) is derived from this plan and it should be absolutely ensured that the appropriate security criteria are included in the PEG.

7.6.2.3 CONFIGURATION MANAGEMENT PLAN (CMP)

Configuration management is a "must" for obtaining a "trusted" system rated division/class B2 or above. The CMP provides both high-level and detailed procedures on baselining the system and identifies components as well as identifying, processing, and controlling changes thereto. The Security Manager will need to serve on the Configuration Control Board to ensure security-relevant issues are adequately addressed. Without stringent hardware and software configuration management, control will be lacking to ensure only authorized and approved changes are made. As a result, the certifying authority will not be able to provide "certification" to the operational user.

7.6.2.4 SOFTWARE DEVELOPMENT SUPPORT PLAN

This is a major support plan for most automated information system acquisitions. All the COMPUSEC requirements and specifications should be described and a detailed approach outlined to satisfy them. This is where the contractor tells how he plans to satisfy the "Orange Book" criteria for the TCB class specified for the acquisition. Chapter 3, Computer Security, provides a brief overview of the software development process.

7.6.2.5 HARDWARE AND SOFTWARE TURNOVER SUPPORT PLAN

This plan is intended to be a detailed listing of tasks to accomplish a "turnover" from the implementing command to the using command. Since implementation and conversion of an automated information system is substantially different than day-to-day operations, the Security Manager should review this plan to ensure security-relevant items have been included (e.g., user s manuals accompany the equipment, personnel are trained and available). The plan should provide a smooth, orderly transition. A checklist should be developed. There needs to be an orchestrated effort among all participants, or a high risk of a security breach at "start-up" will exist.

7.6.2.6 TEST AND EVALUATION MASTER PLAN (TEMP)

This plan is so critical that a separate chapter of this document, Chapter 5, Security Test and Evaluation, was written about security testing.

7.6.2.7 QUALITY ASSURANCE SUPPORT PLAN

Proper quality assurance is a prerequisite to an automated information system. This is true for hardware, software, and all supporting documentation. DoD-STD-2168, "Defense System Software Quality Program" is a valuable guide for software and outlines the quality assurance program. This document and the Quality Assurance Plan for security-relevant items need to be reviewed.

7.6.3 SUPPORT PLANS RELATED TO THE CONCEPT OF MAINTENANCE

This group of support plans is known as the Integrated Logistics Support Plan (ILSP). The plans are designed to support the performance of analyses which relate reliability, maintainability, and supportability to the operational requirements. Security must be considered in these analyses as an operational requirement. The Security Manager should attend all ILS reviews. DoD Instruction 5000.2 (Part 7A) discusses integrated logistic support and is the basic ILSP directive. DoD 5000.2-M (Parts 4C and 15) detail how to determine Life-Cycle Costs (LCC). Also note that security issues should be factored into the total life-cycle costs for the acquisition.

7.6.3.1 MAINTENANCE PLANNING `SUPPORT PLAN

Adequate maintenance is necessary to ensure the system will operate as intended. This plan should establish how many levels of maintenance will be performed and how they will be accomplished (e.g., cleared maintenance personnel, dial-up diagnostics, and warranty repairs).

7.6.3.2 SUPPLY SUPPORT PLAN

Ensuring a fully functional supply pipeline is another essential task. The Security Manager should specify how critical security-relevant parts will be spared and which ones will be required to achieve a stated level of performance. This is especially true for Class A1 systems which require special parts handling. Responsiveness to changes is required in the environment that might change the security requirements, with adjustments as required.

7.6.3.3 SUPPORT EQUIPMENT PLAN

The Security Manager should review and coordinate on this plan if there are specialized test equipment or tool requirements for the system.

7.6.3.4 TECHNICAL DATA SUPPORT PLAN

Some of the security-relevant DIDs generate technical data (e.g., hardware and software specifications). It should be ensured that this support plan has a section for that data.

7.6.3.5 COMPUTER RESOURCES LIFE-CYCLE MANAGEMENT PLAN (CRLCMP)

This is also known as the Computer Resources Support Plan. The Security Manager should review DoD Instruction 5000.2 (Parts 6 and 7) and Federal Information Resources Management Regulation at length. There may be some redundancy between this plan and some of the others, such as configuration management, but better safe than sorry. The Security Manager will be one of the major players in writing this plan. He/she should expect to chair the Computer Security Working Group and to be its representative to the Computer Resources Working Group.

7.6.3.6 PACKING, HANDLING, STORAGE, AND TRANSPORTATION

For highly classified systems (e.g., those dealing with Sensitive Compartmented Information), the Security Manager will need support from the Defense Courier Service (DCOS). For other systems, he/she will also need to consider the security protection measures required for air, road, and sea transport, if they are applicable.

7.7 LIFE-CYCLE PHASES AND DATA DELIVERABLES

There is a lot written about the life-cycle process in the cited references. Studying and comparing these references will reveal that the various milestone charts do not always agree. For example, the life-cycle itself can be divided into different phases, with each phase having a different name, and the individual milestones falling at different points along the time line. Do not let the differences be a source of confusion.

7.7.1 FINEST BREAKDOWN OF LIFE-CYCLE PHASES

First, the maximum set of phases is defined as: determine need, write requirements, develop concepts, validate concept, design, develop, test, deploy/implement, operate, support. Normally, any life-cycle phases will be represented by this list, with some neighboring phases combined and the names altered slightly. The authors of the referenced documents have chosen that combined set which best fits the purpose of the document, but each implicitly pertains to the expanded set. Figure 7-1 provides the acquisition milestones and phases from DoD Instruction 5000.2.

7.7.2 GOVERNMENT/CONTRACTOR PERSONNEL MIX

Keep in mind that each program has a different strategy, and so each may have different functions performed by both the Government and a contractor, or contractors. Contract award(s) could also occur at several points within the life-cycle. It is conceivable that a large and complex program could have an overall life-cycle, while subordinate parts could have their own different, or overlapping life cycles. Software development tends to be particularly volatile, and could also be managed as a separate program. Any program requires a degree of flexibility in adapting the requirements.

7.7.3 DATA DELIVERABLES

In Appendix B to this document, the life-cycle is broken into several distinct periods of time. The data deliverables are shown in a typical time-phased Sequence, with suggested delivery dates keyed to major program milestones. Each program will have its own tailored schedule, but the conceptual flow of deliverables should be similar. The time phases with associated deliverables are described in the following paragraphs.

7.7.3.1 CONCEPT AND DEFINITION PHASE

During this phase, the focus is on defining requirements, evaluating alternative strategies for satisfying requirements and acquiring solutions, and planning for the execution of the program. The Request for Information and Request for Proposal will be released, proposal evaluation and source selection activities will be conducted, and the contract will be awarded.

7.7.3.1.1 EARLY PLANNING DOCUMENTS

Planning documents that were called out in the contract will be delivered to the SPO or PMO for review, and the process will be in full swing. Security should be addressed in nearly every document, but the first one to focus exclusively on security should be the System Security Plan (also called the Security Plan of Accomplishment). The System Security Plan and Operations Security Plans provide the foundation for further security-relevant efforts. They are, therefore, the first to be called out and delivered.

7.7.3.1.2 MORE SPECIFIC PLANS

The next set of security-relevant documents to be delivered are the System Security Concept of Operations, Accreditation Plan, Certification Plan, and Security Test and Evaluation Annex to the Test and Evaluation Master Plan. These plans provide specific information on what the contractor intends to do to satisfy Statement of Work and Security Specification requirements.

7.7.3.1.3 EARLY WORK EFFORT

The third set of security-relevant documents in this initial group reflects the results of the contractor's initial efforts to interpret and satisfy the contractual Statement of Work and Security Specifications. These documents should be the draft Technical Reports covering the Security Audit, the Computer Security Policy Model (when required), the Risk Assessment, and the Cost Benefit Analysis.

7.7.3.2 DESIGN, DEVELOPMENT, AND TEST PHASE

During this phase, the emphasis is on designing, building, and testing the automated information system and its components. Specific solutions to each requirement are spelled out and the automated information system begins to take shape.

7.7.3.2.1 ENGINEERING SPECIFICATIONS

All the major planning documents should now be in-place and approved by the Government. The contractor then begins to document the engineering design of the specific security protection features that are required. The engineering specifications are developed and delivered, in sequence and iteratively, from general to specific. Thus, the next set of documents delivered to the Government should be the "A", "B", and "C" specifications. Once the design specifications are complete and approved, the contractor begins to build the configuration items and other components of the system.

7.7.3.2.2 TEST DOCUMENTATION

Once the security protection feature design configuration begins to take shape, development Security Test Plans are formulated. These plans are reviewed by the Government before actual testing begins. As testing is conducted, the results are documented and provided to the Government in Test Reports. As development testing is completed and the build configuration becomes known, operational Test Plans are formulated. Again, these plans are reviewed by the Government before actual testing begins, with results provided in Test Reports.

7.7.3.2.3 OTHER TECHNICAL DOCUMENTS

Several other security-relevant deliverables fall into this life-cycle phase. They include the Covert Channel Analysis (when required) and Trusted Computing Base Configuration Management Plan. The Certification Support package is also delivered near the end of this phase and includes the results of both development and operational testing, as well as the engineering documentation.

7.7.3.3 OPERATION AND IMPLEMENTATION PHASE

This period corresponds to the time at which an item or system is fielded for use (and continuously used). The automated information system acquisition is complete and the mission user now assumes responsibility for the operation and maintenance of the system.

7.7.3.3.1 USER DOCUMENTATION

The two deliverables in this category are the Trusted Facility Manual and the Security Features Users Guide. These documents describe how the automated information system security protection features are implemented, and how to use them.

7.7.3.3.2 ACCREDITATION SUPPORT

The final security-relevant deliverable is the Accreditation Support package. This culminates the acquisition effort and should result in automated information System accreditation by the Designated Approving Authority (DAA).

7.7.4 USE OF DOD 5010.1 2-L ACQUISITION MANAGEMENT SYSTEM AND DATA REQUIREMENTS CONTROL LIST (AMSDL)

The AMSDL provides an index of DoD Data Item Descriptions (DIDs) that have been approved for general use in defense contracts. The DIDs are used to specify format and content of data from contractors when the information is judged essential to the Government. The AMSDL is the most thorough reference for DIDs for general use during contracting activities. The third book in this guideline series introduces DIDs that will be submitted by NSA for inclusion in the AMSDL.

7.7.4.1 AMSDL ORGANIZATION

The AMSDL has four main sections: 1) Source documents and related DIDs by Data Functional Assignment; 2) Numerical Listing of DIDs; 3) Keyword Index of DIDs; 4) and Canceled or Superseded Listing. The front portion of the AMSDL gives an explanation of how to use each section and its format. These instructions should be reviewed before attempting to use the AMSDL. Unless the DID number is already known, the best bet is to use the Keyword Index to isolate the subject area.

7.7.4.2 WHAT THE AMSDL DOES NOT CONTAIN

The AMSDL does not contain data requirements mandated under other Public Laws, Federal Statutes, or the DoD supplement to the Federal Acquisition Regulation (FAR).

7.7.5 DELIVERABLE MEDIA

Each of the data deliverables called for in the contract will be delivered to the Government in the manner specified by the CDRL. In every case, the contractor should be required to deliver at least one hard copy, with more requested if required. The contractor should also be required to provide the deliverables on floppy diskettes. These diskettes should be prepared using the same word processor that the program office (and ideally the mission user) uses. This will simplify editing and distribution. If formal specification and modeling languages are used, deliverables should be provided in "machine usable" format. Some deliverables may be appropriate for microfiche or microfilm. This determination should be made early, as special equipment is required to prepare and read this type of media. Any electronic deliverables should be ensured by the contractor to be malicious logic free.

7.8 FIELDING THE SYSTEM

7.8.1 PROGRAM MANAGEMENT RESPONSIBILITY TRANSFER

Program Management Responsibility Transfer is the milestone where the Program Management Office turns over the acquired system to the operational user. Ideally, all the program's critical paths merge at this point. However, this ideal is seldom achieved. There are usually some incomplete actions and either the PMO or the mission user must accept responsibility for their completion.

7.8.2 COMPLETION OF CERTIFICATION

Up to this point, the single most significant security achievement has been the certification of the automated information system. At the time of responsibility transfer, the System is turned over to the operational user for accreditation and mission use. With the tools in this guideline, the DAA can be provided with the necessary documentation and assurances needed to accredit the system for use in the operational environment. (See Chapter 6, Certification and Accreditation.)

7.8.3 THE FIELDED SYSTEM

A fielded system is subject to host-tenant support agreements, maintenance management, equipment and supply management, continuing configuration management, hardware and software engineering changes, designation assignment in the inventory, coding and "call-out as a wartime resource, unit reporting, and all the other day-to-day requirements levied upon any automated information system. If the Program Manager has done his job well during acquisition, he/she should not hesitate to accept a follow-on job to operate the system.

7.9 REFERENCES

There are several basic references to have and/or read to gain a detailed understanding of the program management function in the acquisition of secure systems. Most have been introduced previously.

a. "Federal Acquisition Regulation" (FAR) and "DoD FAR Supplement" (DFAR) - This document is the primary regulation in acquisition and must be used as the basis for acquisition activities. The FAR is helpful as well in defining terms and procedures; however, it may require an expert to interpret details.

b. DoD Directive 5000.1, "Defense Acquisition" - After the FAR, this directive is the primary policy and guidance document for DoD acquisitions.

c. DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures" - This instruction is the primary source of acquisition policy and procedures, describing in significant detail the various issues that might arise. The document pertains to both major acquisitions and non major ones. It presents an overview of the acquisition milestone phases and milestones. It then details requirement and affordability issues. In typical Automated Information System acquisition it will be found that some of the detail of this document is not applicable.

d. DoD 5000.2-M, "Defense Acquisition Management Documentation and Reports" - This manual is the primary DoD acquisition management source for formats and concepts for documents developed to support the methodologies of DoD Instruction 5000.2.

e. DOD Directive 7920.1, "Life-Cycle Management of Automated Information Systems" This directive specifically outlines the life-cycle program. Enclosure 2 to this document identifies the activities to be completed during the life-cycle development of automated information systems.

f. DoD Directive 5200.28, "Security Requirements for Automated Data Processing Systems" - This directive establishes the procedure for determining minimum security requirements, in particular the defined operating mode and the division/class of DoD 5200.28-STD to be used as a minimum criteria. This document also sets forth the basic requirement for certification, accreditation, and the corresponding support packages.

g. DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria" - These criteria specifically address the security topics to be produced in security documents (e.g., covert channel analysis, security test, trusted facility manual, security features users guide, formal top level specification, and trusted computing base implementations correspondence issues).

h. DoD-STD-21 67A, "Defense System Software Development" - This standard defines the software development life-cycle and then links it to products, reviews, audits, and baselines.

i. DoD-STD-7935A7 "Automated Information System (AIS) Documentation Standards" - This standard identifies many of the documents that must be produced during design, development, and test.

j. NCSC-TG-006, "A Guide to Understanding Configuration Management in Trusted Systems."

k. NCSC-TG-007, "A Guide to Understanding Design Documentation in Trusted Systems."

l. NCSC-TG-008, "A Guide to Understanding Trusted Distribution in Trusted Systems."

m. NCSC-TG-015 "A Guide to Understanding Trusted Facility Management."

n. NCSC-TG-024, Version-1

Vol 1/4, "A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements," (this document)

Vol 2/4, "A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators," (draft)

Vol 3/4, "A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial," (draft)

Vol 4/4, "A Guide to Procurement of Trusted Systems: How to Evaluate a

Bidder's Proposal Document - An Aid to Procurement Initiators and Contractors" (draft)

o. NCSC-TG-026, "A Guide to Writing the Security Features User's Guide for Trusted Systems."

p. MIL-STD-483A, "Configuration Management Practices for Systems, Equipment, Munitions, and Computer Software.

q. MlL-STD-490A, "Specification Practices."

r. MIL-STD-499B (Draft), "Systems Engineering."

s. DoD 5010.1 2-L, "Acquisition Management Systems and Data Requirements Control Listing."

t. "Information Systems Security Products and Services Catalogue," Prepared by the NSA (Published Quarterly).

u. DoD-STD-21 68," Defense System Software Quality Program."

v. "Federal Information Resources Management Regulation," General Services Administration, 41 CFR 201.

w. DoD Instruction 7920.2, "Automated Information Systems (AIS) Life-Cycle Management Review and Milestone Approval Procedure.

x. DoD 7920.2-M, "Automated Information Systems (AIS) Life-Cycle Manual."

y. DoD Instruction 7920.4, "Baselining of Automated Information Systems (AIS)."

z. DoD 7950.t-M, "Defense Automation Resources Management Manual."

APPENDIX A HISTORICAL BASIS

A.1 INTRODUCTION

A large body of policy is available in the form of regulations, directives, Presidential Executive Orders, and Office of Management and Budget Circulars. This policy serves as a basis for the procedures to handle and process Federal information, particularly classified information. Section 7 of DoD 5200.28-STD "Trusted Computer System Evaluation Criteria," is entitled "The Relationship Between Policy and the Criteria." That section identifies much of the preceding policy and discusses its relationship to establishing control objectives for computer security. Program Managers should familiarize themselves with both the Introduction to DoD 5200.28-STD and Section 7, because the basic documents discussed will be encountered again and again in security literature.

A.2 DISCUSSED IN THE ORANGE BOOK

The following is a brief summary of the most important historical references discussed in section 7 of DoD 5200.28-STD:

a. Brooks Act of 1965 (Public Law 89-306), (Title 40, United States Code, Section 759), "Automatic Data Processing Equipment" - This act, and the amendments thereto, vested in the Administrator of General Services the authority and the responsibility for the acquisition of all automatic data processing equipment (ADPE) and telecommunications resources, unless specifically exempted. GSA relegates that authority to other agencies through delegations of procurement authority (DPAs) (regulatory delegations, specific agency delegations, or specific acquisition delegations).

b. The Nunn-Warner Amendment (or Warner Amendment) to the Brooks Act (Title 10, United States Code, Section 2315), "Law Inapplicable to the Procurement of Automatic Data Processing Equipment and Services for Certain Defense Purposes" - This amendment specifically exempted DoD acquisitions of Mission Critical Computer Resources (MCCR) from the DPA requirement.

c. Ware, W.H., ed., "Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security," AD-A07661 7/0, Rand Corporation, February 1970, reissued October 1979 - This is a report of the findings of a 1967 task force. It contains policy and technical recommendations to reduce threat of compromise of classified information.

d. OMB Circular Number A-71 Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems," July 1978 - This circular requires each Federal agency to implement a computer security program and defines a minimum set of controls to be incorporated into such programs. (This document was superseded by OMB Circular Number A-I 30, see section A.3.c.)

e. Executive Order 12356, "National Security Information," April 6, 1982 - This document established the high-level security initiative. It is expected to be followed by the Secretary of Defense and others.

f. DoD 5200.1-R, "Information Security Program Regulation," August 1982 and

June 1986 - This regulation established policy for the safeguarding of classified, sensitive unclassified, and unclassified information processed in AIS.

g. DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information" - This manual provided security guidance for DoD contractor AISs.

h. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," (previously entitled "Technique and Procedure for Implementing, Deactivating, Testing and Evaluating Secure Resource-Sharing ADP Systems"), December 1972, May 1977, April 1978, March 1988, and 21 May 1988 - This directive is the overall security policy document for systems that process classified data.

i. DoD 5200.28-M, "Automated Information System Security Manual," (previously entitled "Technique and Procedure for Implementing, Deactivating, Testing and Evaluating Secure Resource-Sharing ADP Systems"), January 1973, June 1979, and Draft revision April 1991 - This manual was authorized by and supported DoD Directive 5200.28.

j. DoD Directive 5215.1, "Computer Security Evaluation Center," 25 October 1982 - This directive established the security prOduct evaluation program. NSA has aggressively undertaken the task to study and implement computer security technology. NSA has encouraged the widespread availability of trusted computer products for use by any organization desiring better protection for their sensitive data.

k. OMB Circular Number A-123, "Internal Control Systems," August 1986 - This OMB circular establishes confidence and accountability in the protection of Federal AIS operations from fraud, waste, and abuse. It requires the development of management control plans based on such actions as vulnerability assessments and personnel performance agreements.

l. DoD Directive 7920.1, "Life Cycle Management of Automated Information Systems," October 17, 1978 (updated June 20, 1988) - This directive minimized acquisition cost through life-cycle management according to phases and milestones.

m. DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria" - This document was originally issued as DoD Computer Security Center CSC-STD-001-83 on 15 August 1983, it was reissued 26 December 1985 as a Department of Defense Standard.

A.3 SINCE THE ORANGE BOOK

A few important policy documents have been published since the finalization and subsequent adaptation of DoD 520028-STD in December of 1985, and therefore are not referenced in Section 7 of that document. They include:

a. Update of DoD Directive 5200.28, "Technique and Procedure for Implementing, Deactivating, Testing and Evaluating Secure Resource-Sharing ADP Systems," March 1988 - This update provides minimum security guidelines and more specific guidance for classified and sensitive information protection, specifically the specification of C2 criteria under DoD 5200.28-STD by 1992.

b. National Security Decision Directive 145,17 December 1984 - This directive was developed by the policy and organizational structure steering group, Secretary of Defense for Automated Information. This document was replaced by National Security Directive 42, 5 July 1990.

c. OMB Circular Number A-I 30, "Management of Federal Information Resources," December 1985, Appendix III, "Security of Federal Automated Information Systems" - Superseding OMB Circular A-71,this document requires that systems be approved for processing based on the adequacy of the safeguards. It establishes requirements for the effective and efficient use and management of Federal information resources. It requires that all agency information systems possess a level of security commensurate with the sensitivity of the information and also commensurate with the risk and harm that could result from improper operation. (This document supersedes OMB Circular A-71, see Section A.2.d.)

d. NTISSAM COMPUSEC/1-87, "National Telecommunications and Information Systems Security (NTISS) Advisory Memorandum on Office Automation Security Guideline" - This guideline provides guidance to users of microprocessor-based systems used for such functions as typing, filing, calculating, and sending/receiving electronic mail.

e. Public Law 100-235, "Computer Security Act of 1987," January 1988 - Over 53,000 Federal information systems have been designated as sensitive in compliance with this document. The results of this act are not reflected in the 1988 update to DoD Directive 5200.28. However, they have been reflected in the April 1991 draft revision to DoD 5200.28-M.

APPENDIX B PLAN AND DELIVERABLE DOCUMENT SUMMARIES

B.1 DOCUMENTS RELATED TO FUNCTIONAL AREAS

This appendix provides the common document title, a brief description of the document's purpose, and the regulations that specify the document content and/or govern the document's use.

B.1.1 PLANNING AND FINANCIAL MANAGEMENT DOCUMENTS

Policy and Strategy Documents

Includes National Security Decision Directives, Defense Guidance, and the Five Year Defense Program
DoDI 7045.7, DoDI 7045.14

Program Objective Memorandum (POM)
Provides response to DOD planning documents
DoDI 7045.7, DoDI 7045.14

Program Decision Memorandum
Adjustments to the POM to ensure consistency with DOD guidance
DoDI 7045.7, DoDI 7045.14, DoDI 5000.2 (Sect 3)

Budgets
Budget estimates and the final Budget submitted to Congress
DoDI 7045.7, DoDI 7045.14

Appropriations
Approval by Congress to spend dollars on specific line items, or for specific programs
DoDI 7045.7, DoDI 7045.14

Obligation Authorities
Means of passing funds down from the DoD
DoDi 7045.7, DoDI 7045.14

Program Decision Package (PDP)
Used in Conjunction with budget submissions to explain what is needed, why it is needed, and impact if not funded
DoD] 7045.7, DoD] 7045.14, DoD] 5000.2 (Sect 2,3,4D)

B.1.2 PROGRAM MANAGEMENT DOCUMENTS

Acquisition Decision Memorandum
Approval for a program to move into the next phase
DoDI 5000.2 (Sect 3)

Program Management Directive (PMD)
Provides direction to participating commands and authorizes the program to proceed

Program Management Plan (PMP)

Provides detailed tasking, outlines Organizational structures, and prescribes detailed support plans
DOD 5000.2 (Sect 2, 5B, 10C, 11)

Configuration Management Plan (CMP)
Describes responsibilities, resources, and approach to configuration management
DoDI 5000.2 (Sect 9A)

Source Selection Plan (SSP)
Describes responsibilities, resources, and approach to source selection
DoDI 5000.2 (Sect 2,5,1 0B)

Proposal Evaluation Guide (PEG)
Describes the step-by-step procedure and criteria to be used in proposal evaluation
DoDI 5000.2 (Sect lOB)

Acquisition Program Baselines
Represents the objectives and thresholds for the system to be produced and fielded
DoDI 5000.2 (Sect 11), DoD 5000.2-M

Computer Resources Life-Cycle Management Plan (CRLCMP)
Describes computer resources development strategy, software support concept, and identifies applicable directives
DoD 5000.2 (Sect 6D, 7A)

Test and Evaluation Master Plan (TEMP)
Describes the overall testing plan, with separate annexes identifying functional area test plans
DoDI 5000.2 (Sect 6, 7B, 8), DoD 5200.2-M, DoD-STD-7935A, DoD-STD-21 67A

Integrated Logistics Support Plan (ILSP)
Describes maintenance, supply, training, transportation, and other logistics approaches
DoDI 5000.2 (Sect 6F, 7A)

Award Conference Minutes
Documents initial discussions with successful offerors

Post Award Debriefing Minutes
Documents lessons learned and highlights of deliberations as briefed to offerors

B.1.3 MISSION USER DOCUMENTS

Mission Need Statement (MNS)

Describes a requirement or deficiency and justifies exploring alternative solutions
DoDI 5000.2 (Sect 3, 4B), DoD 5000.2-M

Justification for Major Systems New Start
Describes operational needs, projected threats, and plans to identify and research alternative concepts for POM submission
DoDD 5000.1

System Threat Assessment Report (STAR)
Prepared by the intelligence community, validated by the Defense Intelligence Agency
DoDI 5000.2 (Sect 4A, 4C), DoD 5000.2-M

Operational Requirements Document
Contains performance and related operational parameters for the proposed concept or system
DoDI 5000.2 (Sect 40, 4C), DoD 5000.2-M, DoD-STD-21 67A, DoD-STD-7935A

Secure Automated Information System Requirements Document
Describes required security capability, justifies the need, and serves as the validation and approval document
DoDI 5000.2 (Sect 5F, 6J), DoDD 5200.28, DoD 5200.1 R

Functional Description ("A" Specification)
Describes the broad functional requirements of the system, equipment, or software in terms of capabilities
DoD-STD-7935A, MlL-STD-499, MlL-STD-21 67A, MlL-H-46855, MlL-STD-1 521

System/Subsystem Specification ("B" specifications)
Describes component parts of the system in terms of functions and features
DoD-STD-7935A, MlL-STD-499, MlL-STD-21 67A, MlL-H-46855, MlL-STD-1 521

Unit Specification ("C" Specification)
Describes the "as built" configuration in terms of detailed design information
DoD-STD-7935A, MlL-STD-499, MlL-STD-21 67A, MlL-H-46855, MlL-STD-1 521

B.1.4 CONTRACTING DOCUMENTS

Information for Bid
Used for acquisitions of standard commercial, off-the-shelf items
FAR, DFAR

Request for Quote (RFQ)
A request for pricing information
FAR, DFAR

Request for Information (RFI)
Precedes a Request for Proposal and is really a draft RFP issued to receive feedback from industry
FAR, DFAR

Request for Proposal (RFP)
Used for automated information system oriented acquisitions (contents below are listed by the standard section letter designation)
FAR, DFAR

A. Cover Sheet and Contract FOrm
General information for offerors and table Of cOntents

B. Supplies of Services and Prices/Cost
List of contract line items to be acquired and a price table

C. Description-Specification
Description of the line items being acquired including specificatiOn (trusted system language of this section is discussed in Volume 2 of this guideline series)
DoD-STD-7935A

and Statement of Work (SOW)
Description of work to be accomplished.
DoDI 5000.2 (Sect 6A, 6B, 6D, 6H, 6J), MIL-HDBK-245B

D. Packaging and Marking
Describes how to mark and package deliverables

E. Inspection and Acceptance
Explains how and where deliverables will be tested, certified and accepted

F. Deliveries and Performance
Describes where and when delivery shall occur, including who pays shipping cost

G. Contract Administration Data
Administrative information

H. Special Contract Requirements
Points of contact, billing and delivery order information

I. Contract Clauses
Clauses unique and specially tailored for the acquisition

J. List of Documents, Exhibits, and Other Attachments
CDRLS (DD Form 1423), DIDs (DD Form 1664), DD Form 254, Glossary and other attachments unique to the project (DIDs are the topic of Volume 3 of this guideline series)
DoD 501 0-I 2-L

K. Representations, Certifications, and other Statements of the Offeror
Information to be supplied by the offeror about general conduct of business

L. Instructions, Conditions, and Notices to Offerors
Administrative information, conditions, proposal preparation instructions, cost/price tables, technical questionnaires

M. Proposal Evaluation Factors
Basis of award and how proposals will be validated and evaluated (discussed in Volume 4 of this guideline series)

DoD 5000.2 (Sect 10)

B.2 SUPPORT PLANS RELATED TO CONCEPTS

B.2.1 SUPPORT PLANS RELATED TO THE CONCEPT OF OPERATIONS

Survivability Support Plan
Describes the ability to survive, reconstitute, and sustain operations

Training Support Plan
Includes a module on system security that provides the system administrator, security officer, maintainers, and users training commensurate with their system involvement

B.2.2 SUPPORT PLANS RELATED TO THE CONCEPT OF ENGINEERING

Contracting and Acquisition Support Plan
Indicates security manager participation in the Data Call and the Data Requirements Review Board, acknowledges that security is a driving cost factor, identifies the technical representative on security issues, and reserves a place in the RFP SOW for security requirements and specifications
MlL-HDBK-245B, FAR

Source Selection Plan
Describes organization, roles, responsibilities, and functions of the Source Selection Evaluation Board and outlines award criteria and "evaluation factors" and scoring methodology

Configuration Management Plan (CMP)
Provides procedures on baselining the system and its components as well as identifying, processing, and controlling changes

Software Development Support Plan
Describes COMPUSEC requirements and the approach to satisfy them

Hardware and Software Turnover Support Plan
Includes security-relevant items (e.g., user's manuals accompany the equipment, personnel are trained and available) to provide a smooth, orderly transition

Test and Evaluation Master Plan (TEMP)
Detailed plan that includes Security Test and Evaluation

Quality Assurance Support Plan
Outlines the quality assurance program for security-relevant items

B.2.3 SUPPORT PLANS RELATED TO THE CONCEPT OF MAINTENANCE

Maintenance Planning Support Plan
Establishes how many levels of maintenance will be performed and how they will be accomplished (e.g., cleared maintenance personnel, dial-up diagnostics, warranty repairs)

Supply Support Plan

Specifies how critical security-relevant parts will be spared and which ones will be required to achieve a stated level of performance

Support Equipment Plan

Includes specialized test equipment or tool requirements

Technical Data Support Plan

Must contain security-relevant technical data (e.g., hardware and software specifications)

Computer Resources Life-Cycle Management Plan

Provides information of security use of computer resources and security implications of overall use as a denial of service issue

Packing, Handling, Storage, and Transportation Support Plan

Provides support to classified systems requiring support from the Defense Courier Service (DCOS) and other systems and also to consider the security protection measures required for air, road, and sea mobility

B.3 LIFE-CYCLE PHASES AND DATA DELIVERABLES

Most (or all) of these documents are required for major systems development. They might be developed by the Government or are required by the contract. Documents that are iterated throughout the system life-cycle such as security policy and risk analysis are not included. For smaller systems the functionality of each document is still required although several might be combined. Each topic addressed needs to be clearly delineated however.

Delivery dates are in days and are only examples. The legend for delivery date baselines is as follows:

CA Contract Award

MS2 Milestone 2 Completion of Concept and Definition Phase

SDR System Design Review (Functional Baseline)

SSR Subsystem Requirement Review (Allocated Baseline)

CDR Critical Design Review (Design Baseline)

MS3 Milestone 3 Completion of Design, Development and Test

IOC Initial Operational Capability

B.3.1 CONCEPT AND DEFINITION PHASE

System Security Plan

CA + 30

Operations Security Plan

CA + 30

System Security Concept of Operations

CA + 120

Accreditation Plan

CA + 120

Certification Plan

CA + 120

Security Test and Evaluation Annex to the TEMP

CA + 120

Security Audit

CA + 120

Security Policy Model (Informal or Formal)

MS2 - 30

Risk Analysis/Assessment

MS2-30

Economic Assessment

MS2-30

B.3.2 DESIGN, DEVELOPMENT, AND TEST PHASE

Descriptive TOp-Level Specification

M52 + 30

Formal Top-Level Specification Verification Tools

SDR-30

Interface Requirements Specification (Can be part of "C" Spec)

SDR - 30

Database Design Document (Can be part of "C" Spec)

SDR-30

Clandestine Vulnerability Analysis

SSR-30

Formal Top-Level Specification

SSR-30

Functional Description ("A" Spec)

SSR-30

System/Subsystem Specification

CDR-30

Covert Channel Analysis

CDR-30

Trusted Computing Base Implementation Correspondence

CDR + 30

Test Plans

SDR/CDR + 30

Test Reports

TEST + 30

Certification Support Package

MS3 - 30

B.3.3 OPERATION AND IMPLEMENTATION PHASE (USER DOCUMENTATION)

Trusted Facility Manual

MS3 + 30

Security Features Users Guide

MS3 + 30

Accreditation Support Package

IOC - 30

B.4 DOCUMENT SUMMARY

"A" Specification

(See Functional Description)

Chapter: 2,3,7,01,03

Reference: DoD-STD-21 67A, DoD-STD-7935A, DoD 5200.28-STD

Accreditation Plan

Chapter: 6,7, 03

Reference: DoDD 5200.28, DoD 5200.28-M, FIPS PUB 102

Accreditation Support Package

Chapter: 6, 03

Reference: DoD 5200.28-M

Acquisition Decision Memorandum

Chapter: 2, 01

Reference: DODI 5000.2 (Sect 3)

Acquisition Program Baselines

Chapter: 2, 01

Reference: DoD 5000.2 (Sect 11), DoD 5000.2-M

Acquisition System Protection Plan

Chapter: 4

Reference: DoDI 5000.2 (Sect 5F)

Appropriations

Chapter: 2, 01

Reference: DoD 7045.7, DoDI 7045.14

"B" Specification

(See System/Subsystem Specification)

Budgets

Chapter: 2, B1

Reference: DoD 7045.7, DoDI 7045.14

"C" Specification

(See Unit Specification)

Certification Plan

Chapter: 6,7, 03

Reference: DoDD 5200.28, DoD 5200.28-M, FIPS PUB 102

Certification Support Package

Chapter: B3

Reference: DoD 5200.28-M

Clandestine Vulnerability Analysis

Chapter: 4,6, 03

Reference: Threat assessment report from the Director of the Defense Intelligence Agency (DIA)

Computer Resources Life-Cycle Management Plan

(Also the Computer Resources Integrated Support Document)

Chapter: 2,7, B1, B2

Reference: DoDI 5000.2 (Sect 6D,7A), DoDD 7920.1

Concept of Operations

(See System Security Concept of Operations)

Chapter: 7

Reference: DoD-STD-21 67A, DoD-STD-7935A

Concept of Engineering

Chapter: 7

Reference: DoD 5000.2 (Sect 6), MlL-STD 499

Concept of Maintenance

(See Maintenance Procedures for Security Relevant HW and SW)

Chapter: 7

Reference: DoDI 5000.2 (Sect 6C)

Configuration Management Plan

Chapter: 2,7, B1, B2

Reference: DoD 5000.2(9A), DoD 5200.28-STD, DoD-STD-2I 67A,

DoD-STD-480

Contingency Plan

Chapter: 6

Reference: DOD 5200.28-M

Contracting and Acquisition Support Plan

(Acquisition Strategy Report DOD 5000.2-M)

Chapter: 7, B2

Reference: MlL-HDBK-245B, FAR

Cost Benefit Analysis

(Also called Economic Assessment)

Chapter: 4,6

Reference: DoD 5000.2 (Sect 3,5,10), DoD 5000.2-M, DoDD 5000.4

Covert Channel Analysis Report

DID: Guideline Series Volume 3

Chapter: 3,6, B3

Reference: DoD 5200.28-STD

Database Design Document

(Part of "C" Spec Requirements)

Chapter: B3

Reference: DoD 5200.28-STD, DoD-STD-7935A

Description Specification

(Part of the RFP. Often it is the Functional Description.)

Chapter: 2

Reference: DoD-STD-7935A, Guideline Series Volume 2

Descriptive Top-Level Specification

DID: Guideline Series Volume 3

Chapter: 3, 03

Reference: DoD 5200.28-STD

Design Specification

DID: Guideline Series Volume 3

Chapter: 3, 03

Reference: DoD 5200.28-STD, NCSC-TG-005, NCSC-TG-007, NCSC-TG-008, NCSC-TG-009, NCSC-TG-021

Formal Security Policy Model

DID: Guideline Series Volume 3

Chapter: 3, 02, 03

Reference: DoD 5200.28-STD

Formal Top-Level Specification

DID: Guideline Series Volume 3

Chapter: 3, 03

Reference: DoD 5200.28-STD

Formal Top-Level Specification Verification Tools

Chapter: 03

Reference: NCSC-TG-01 4

Functional Description

(Also called "A" Specification and Top Level Specification)

(In the RFP this is often the Description-Specification)

DID: DoD 501 0-1 2-L, AMSDL

Chapter: 2,3,7,01, B3

Reference: DoD-STD-7935A, MlL-STD-499, MlL-STD-21 67A,MlL-H-46855, MlL-STD-1 521

Hardware and Software Turnover Support Plan

(Trusted Distribution)

Chapter: 7, 02

Reference: DoD 5200.28-STD

Informal Security Policy Model

DID: Guideline Series Volume 3

Chapter: 3, 02, B3

Reference: DoD 5200.28-STD

Information for Bid

Chapter: 2, 01

Reference: FAR, DFAR

Installation Procedures for Security Relevant Hardware and Software

Chapter: 6,7

Reference: Vendor Documentation

Instructions, Conditions, and Notices to Offerors

(Part of RFP)

Chapter: 2, B1

Reference: FAR, DFAR

Integrated Logistics Support Plan

(Also the Supply Support Plan)

Chapter: 2,7, B2

Reference: DoDI 5000.2 (Sect 6F, 7A)

Interface Requirements Specification

(Part of "C" Spec Requirements)

Chapter: B2

Reference: DoD-STD-7935A

Justification for Major System New Start

Chapter: 2, BI

Reference: DoDD 5000.1

List of Documents, Exhibits, and Other Attachments

(Part of RFP)

Chapter: 2, BI

Reference: DoD 5010-12-L, FAR, DFAR, Guideline Series Volume 2

Maintenance Planning Support Plan

Chapter: 7, B2

Reference: DoDI 5000.2 (Sect 6)

Maintenance Procedures for Security Relevant Hardware and Software

(Maintenance Manual DoD-STD-7935A)

Chapter: 6

Reference: DoDI 5000.2 (Sect 6)

Mission Impact Statement

Chapter: 6

Reference: DoDI 5000.2 (Sect 3,4)

Mission Need Statement

(Also called Statement of Need)

Chapter: 2, 7, B1

Reference: DoDI 5000.2 (Sect 3,4B), DoD 5000.2-M

Obligation Authority

Chapter: 2, B1

Reference: DoDI 7045.7, DoDI 7045.14

Operational Requirements Document

(Also see Secure AlS Requirements Document)

Chapter: 6, B1

Reference: DoDI 5000.2 (Sect 4B,4C), DoD 5000.2-M, DoD-STD-2167A,

DoD-STD-7935A

Packing, Handling, Storage, and Transportation Support Plan

Chapter: 7, 02

Reference: DODD 5200.1-R

Philosophy of Protection Report

DID: Guideline Series Volume 3

Chapter: 3

Reference: DoD 5200.28-STD

Program Decision Memorandum

Chapter: 2, 01

Reference: DoDI 7045.7, DoDI 7045.14, DoDI 5000.2 (Sect 3)

Program Decision Package

Chapter: 2, 01

Reference: DoDI 7045.7, DoD 7045.14, DOD 5000.2 (Sect 2,3,4D)

Program Funding Profile

Chapter: 7

Reference: DoDI 7045.7, DoD 7045.14, DoD 5000.2-M

Program Management Directive

Chapter: 2,5, 7, B1

Reference: DoDI 5000.2(2, 50,10C, 11E)

Program Management Plan

(See also System Security Plan)

Chapter: 5, 01

Reference: DoDI 5000.2(2, 5B, 10C, 11E)

Program Objective Memorandum

Chapter: 2, 01

Reference: DoDI 7045.7, DoDI 7045.14

Program Status Reporting

Chapter: 7

Reference: DoD 5000.2-M

Proposal Evaluation Guide

Chapter: 2

Reference: DoDI 5000.2 (Sect 100), Guideline Series Volume 4, FAR, DFAR

Proposal Evaluation Factors

(Part of RFP)

Chapter: 01

Reference: DoDI 5000.2 (Sect 10), Guideline Series Volume 4

Quality Assurance Support Plan

Chapter: 7, 02

Reference: DoD 5000.2 (Sect 6P)

Request for Information

Chapter: 2, 01

Reference: FAR, DFAR

Request for Proposal

Chapter: 2, B1

Reference: FAR, DFAR

Request for Quote

Chapter: 2, B1

Reference: FAR, DFAR

Risk Analysis

Chapter: 4, B3

Reference: DoD 5200.28-M, FIPS PUB 65

Risk Assessment

Chapter: 4, B3

Reference: DoDD 5200.28

Secure Automated Information System Requirements Document

Chapter: 6

Reference: DoD 5000.2 (Sect SF,6J), DoDD 5200.28, DoD 5200.1 R

Security Audit (Internal and External)

Chapter: B3

Reference: NCSC-TG-001

Security Features User's Guide

(Also Security Procedures in DoD 5200.28-M)

DID: Guideline Series Volume 3

Chapter: 3,6,7, B3

Reference: DoD 5200.28-STD, NCSC-TG-026

Security Policy

Chapter: 3

Reference: DOD 5200.28-M, DoD 5200.28-STD, FlRMR 20121.302

Security Policy Model

(See Formal Security Policy Model)

(See Informal Security Policy Model)

Chapter: 3, B2, B3

Reference: DoD 5200.28-STD

Security Test and Evaluation Annex to the TEMP

Chapter: 2,5, 6,7, B1, B2, B3

Reference: DoDD 5000.2-M

Security Test Plan

DID: Guideline Series Volume 3

Chapter: 2, 5,6,7, B3

Reference: DOD 5200.28-STD, DoD-STD-2167A, DoD-STD-7935A

Software Development Support Plan

Chapter: 7, B2

Reference: DoDI 5000.2 (Sect 6D), DoD-STD-2167A

Source Selection Plan

Chapter: 2,7, 01, B2

Reference: DoDI 5000.2 (Sect 2, 5, 100), DOD 5000.2-M

Special Contract Requirements

(Part of RFP)

Chapter: 2,01

Reference: FAR, DFAR

Statement of Work

(Part of RFP)

Chapter: 2,01

Reference: DoDI 5000.2 (Sect 6A,6B,6D,6H,6J), MlL-HDBK-245B, FAR, DFAR

Support Equipment Plan

Chapter: 7, 02

Reference:

Survivability Support Plan

(Also called the Endurability Support Plan)

Chapter: 7,02

Reference: DoDI 5000.2

System Security Concept of Operations

Chapter: 4,6,7, 03

Reference: DoD-STD-2167A

System Security Plan

(Security Plan of Accomplishment in DODI 5000.2 Sect. 5F)

Chapter: 4,6

Reference: DOD 5200.28-STD, DoDI 5000.2 (Sect 6), OMBB 90-08

System/Subsystem Specification

(Also called "B" Specification)

(Also called Software Subsystem Specification)

(See Design Specification)

DID: DoD 5010-1 2-L, AMSDL

Chapter: 2,3,7, 02, B3

Reference: DoD-STD-7935A, MlL-STD-499, MlL-STD-2167A, MlL-H-46855, MlL-STD-1521, DoDI 5000.2 (Sect 6)

System Threat Assessment Report

Chapter: 2,4, B1

Reference: DoDI 5000.2 (Sect 4A, 4C), DoD 5000.2-M

Technical Data Support Plan

Chapter: 7,02

Reference:

Test and Evaluation Master Plan

(See also Security Test and Evaluation Annex to the TEMP)

Chapter: 2,5,6,7, 01, 02, 03

Reference: DoDI 5000.2 (Sect 6F, 6H, 6I, 7B, 7H, 8), DoD 5200.2-M, DoD-STD-7935A, DoD-STD-2167A

Test Plan

(See Security Test Plan)

Test Procedures

DID: DoD 5010-12-L, DIN DTI 8603

Chapter: 5

Reference: DoD 5200.28-STD, DoD-STD-2167A, DoD-STD-7935A

Test Reports

DID: DoD 50I0-12-L, AMSDL, DIN DTI 8609

Chapter: 5, 6, 7, B3

Reference: DoD-STD-21 67A, DoD-STD-7935A

Training Support Plan

(Part of Human System Integration Plan in DoD 5000.2 (Sect. 7B))

Chapter: 7, B2

Reference: NIST SP 500-172

Trusted Computing Base Configuration Management Plan

DID: Guideline Series Volume 3

Chapter: 7, B3

Reference: DoD 5200.28-STD, NCSC-TG-006

Trusted Computing Base Verification Report

DID: Guideline Series Volume 3

Chapter: 6, B3

Reference: DoD 5200.28-STD

Trusted Facility Manual

DID: Guideline Series Volume 3

Chapter: 3,6,7, B3

Reference: DoD 5200.28-STD, NCSC-TG-015

Unit Specification

(Also called "C" Specification

(Also called Software Unit Specification)

(See Design Specification)

DID: DoD 5010-12-L, AMSDL

Chapter: 2,3,7, B1

Reference: DoD-STD-7935A, MlL-STD-499, MIL-STD-2167A,MIL-H-46855,

MIL-STD-1521

APPENDIX C BIBLIOGRAPHY

C.1 WORKING BIBLIOGRAPHY

"Acquisition of Information Resources; Overview Guide," U.S. General Services Administration, January 1990

Cheheyl, M., M. Gasser, G. Huff, J. Millen, "Verifying Security," ACM Computing Surveys, Volume 13, Number 3, September 1983

"Competition in Contracting Act of 1984" (CICA)

CSC-STD-002-85, "Department of Defense (DoD) Password Management Guideline," April 12,1985

CSC-STD-003-85, "Computer Security Requirements - Guidance for Applying the Department of Defense (DOD) Trusted Computer System Evaluation Criteria (TCSEC) to Specific Environments," June 25,1985 (Updated as enclosure 4 of DoD Directive 5200.28)

CSC-STD-004-85 "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense (DOD) Trusted Computer System Evaluation Criteria (TCSEC) to Specific Environments," June 25, 1985

DIAR 55-3, "System Threat Assessment Report" (STAR)

DoD-STD-480, "Configuration Control - Engineering Changes, Deviations and Waivers"

DoD-STD-2167A," Defense System Software Development," February 29,1988

DoD-STD-2168, "Defense System Software Quality Program"

DoD Directive 3020.26, "Continuity of Operations Policies and Planning," October 24,1985

DoD Directive 3405.1, "Computer Programming Language Policy," April 2,1987

DoD 4245.7-M, "Transition from Development to Production, September 1985

DOD Directive 5000.1, "Defense Acquisition," February 23,1991

DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23,1991

DOD 5000.2-M, "Defense Acquisition Management Documentation and Reports," February 1991

DoD Directive 5000.4, "OSD Cost Analysis Improvement Group," October 30,1980

DoD Instruction 5000.33, "Uniform Budget/Cost Terms and Definitions," August 15, 1977

DoD 5010.12-L, "Acquisition Management Systems and Data Requirements Control List," October 1,1990

DoD 5010.38," Internal Management Control Program," April 14, 1987

DoD Directive 5200.1, "DoD Information Security Program," June 7,1982

DOD 5200.1-R, "Information Security Program Regulation," August 1982, June 1986, Change June 27,1988

DoD 5200.2-R, "DoD Personnel Security Program," January 1987

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21,1988

DoD 5200.28-M, (Draft) "Automated Information System Security Manual," April 29, 1991

DOD 5200.28-STD, "DoD Trusted System Evaluation Criteria," December 26,1985

DoD Directive 5215.1, "Computer Security Evaluation Center," October 25,1982

DoD Instruction 5215.2, "Computer Security Technical Vulnerability Program (CSTVRP)," September 2,1986

DOD Directive 5220.6, "Defense Industrial Personnel Security Clearance and Review Program," August 12,1985, Change April 9,1986

DOD Directive 5220.22, "Industrial Security Program," December 8,1980

DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information" January 1991

DoD 5220.22-R, "Industrial Security Regulation," December 1985

DoD Instruction 7041.3, "Economic Analysis and Program Evaluation for Resource Management," October 18,1972

DoD Instruction 7045.7, "Implementation of the Planning, Programming, and Budgeting System (PPBS)," May 23,1984

DoD Instruction 7045.14, "The Planning, Programming and Budgeting System (PPBS)," May 22,1984

DoD Instruction 7110.1, "DoD Budget Guidance," October 30,1980

DoD 7110.1-M, "DoD Budget Guidance Manual," May 1990

DoD Directive 7740.2, "Automated Information System Strategic Planning," July 29, 1987

DoD Directive 7750.5, "Management and Control of Information Requirements," August 7,1986

DoD Directive 7920.1, "Life-Cycle Management of Automated Information Systems (AIS)," June 20,1988

DoD Instruction 7920.2, "Automated Information Systems (AS) Life-Cycle Management Review and Milestone Approval Procedure," March 7,1990

DoD 7920.2-M, "Automated Information Systems (AS) Life-Cycle Manual"

DoD Instruction 7920.4, "Baselining of Automated Information Systems (AIS)," March 21, 1988

DoD-STD-7935A, "Automated Information System (AIS) Documentation Standards," February 15,1983

DoD 7950.1-M, "Defense Automation Resources Management Manual," September 1988

Executive Order 12356," National Security Information," April 6,1982

"Federal Acquisition Regulation" (FAR), Title 48,1990 Edition Issued by GSA, DoD and NlST and "DoD FAR Supplement" (DFAR)

"Federal Information Resources Management Regulation (FlRMR)," General Services Administration (41 CFR Ch 201)

"Financial Integrity Act of 1982"

FIPS PUB 31, "Guidelines for ADP Physical Security and Risk Management," U.S. Department of Commerce, NBS, June 1974

FIPS PUB 39, "Glossary for Computer System Security," U.S. Department of Commerce, NBS, February 15,1976

FIPS PUB 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," U.S. Department of Commerce, NBS

FIPS PUB 48, "Guidelines on Evaluation of Techniques for Automated Personal Identification," U.S. Department of Commerce, NBS, April 1,1977

FIPS PUB 65, "Guideline for Automatic Data Processing Risk Analysis," U.S. Department of Commerce, NBS, August 1,1979

FIPS PUB 73, "Guidelines for Security of Computer Applications," U.S. Department of Commerce, NBS, June 30,1980

FIPS PUB 83, "Guideline for User Authentication Techniques for Computer Network Access," U.S. Department of Commerce, NBS

FIPS PUB 102, "Guidelines for Computer Security Certification and Accreditation," U.S. Department of Commerce, NBS, September 27,1983

FIPS PUB 112, "Password Usage Standard," U.S. Department of Commerce, NBS, May 30,1985

Gasser, M., Buildinq a Secure Computer System, Van Nostrand Reinhold, New York, 1988

GSA Index of Federal Specifications, Standards and Commercial Item Descriptions

Gilbert, Irene, "Guide for Selecting Automated Risk Analysis Tools," Special Publication 500-174, National Institute of Standards and Technology, October 1989

Guttman, Barbara, "Computer Security Requirements in Procurement, A Guide for Procurement lnitiators, Contracting Officers, and Computer Security Officials," NIST Document, Limited External Review Draft, April 22,1991

IMTEC-88-11 and 11S, "Agencies Overlook Security Controls During Development, Government Accounting Office Report to Chairman of the Committee on Science, Space and Technology, House of Representatives," 1988

"Information Systems Security Products and Services Catalogue," Prepared by the National Security Agency, (Published Quarterly)

ISO 7498/Part 2 - "Security Architecture," ISO/TC 97/ SC21/N1528/WS1 Ad Hoc Group on Security, Project, 97.21.18, September 1986

Litant, T. F., "The Automated Threat Assessment Methodology," MITRE Corporation, August 1982

MIL-HDBK-245B, "Preparation of Statements of Work"

MIL-STD-481, "Configuration Control, Engineering Changes, Deviations and Waivers"

MIL-STD-483A, "Configuration Management Practices for Systems, Equipment, Munitions, and Computer Software"

MIL-STD-490A, "Specification Practices"

MIL-STD-499, "Engineering Management"

MlL-STD-4990 (Draft), "Systems Engineering"

MlL-STD-881A, "Work Breakdown Structures for Defense Material Items"

MlL-STD-1521A, "Technical Review and Audits for Systems, Equipments and Computer Programs," 1 June 1976, with Notice 1, 29 September 1978, with Notice 2, December 21,1981

MIL-STD-1 777, "Internet Protocol"

MlL-STD-1 778, "Transmission Control Protocol"

MIL-STD-1 785, "System Security Engineering Program Management Requirements," September 1989

MIL-H-46855, "Human Engineering Requirements for Military Systems, Equipment, and Facilities"

"Model Framework for Management Control Over Automated Information Systems," President's Council on Management Improvement and the Presidents Council on Integrity and Efficiency, January 1988

MTR-90W00138, M. Abrams, D. Akers, K. Offing, A. Lee, ,,J. Lovelace, and B. McKenney, `Overview of Security in the Acquisition Process, prepublication copy, The MlTRE Corporation, December 1990

National Institute of Standards and Technology, Special Publications 500-172, "Computer Security Training Guidelines," November 1,1989

Neugent, W., J. Gilligan, L. Hoffman, Z. Ruthberg, "Technology Assessment of Methods for Measuring the Level of Computer Security," NBS Special Publication 500-133, October 1985

NCSC-TG-001,"A Guide to Understanding Audit in Trusted Systems," June 1,1988

NCSC-TG-002, Version 2, "Trusted Product Evaluation, A Guide for Vendors," April 29,1990

NCSC-TG-003, "A Guide to Understanding Discretionary Access Control (DAC) in Trusted Systems," September 30,1987

NCSC-TG-004, "Glossary of Computer Security Terms," October 21,1988

NCSC-TG-005, "Trusted Network Interpretation (TN) of the Trusted Computer System Evaluation Criteria (TCSEC)," July 31,1987

NCSC-TG-006, "A Guide to Understanding Configuration Management in Trusted Systems," March 28,1988

NCSC-TG-007, "A Guide to Understanding Design Documentation in Trusted Systems," October 2,1988

NCSC-TG-008, "A Guide to Understanding Trusted Distribution in Trusted Systems," December 15,1988

NCSC-TG-009, "Computer Security Subsystem Interpretation (CSSI) of the Trusted Computer System Evaluation Criteria (TCSEC)," September 16,1988

NCSC-TG-011, "Trusted Network Interpretation Environments Guideline," August 1, 1990

NCSC-TG-013, "Rating Maintenance Phase, Program Document," June 23,1989

NCSC-TG-014, "Guidelines for Formal Verification Systems," April 1,1989

NCSC-TG-015, "A Guide to Understanding Trusted Facility Management," October 18,1989

NCSC-TG-017, "A Guide to Understanding Identification and Authentication in

Trusted Systems," September 1, 1991

NCSC-TG-018, "A Guide to Understanding Object Reuse in Trusted Systems," July 1992

NCSC-TG-019, "Trusted Product Evaluation Questionnaire," October 16,1989

NCSC-TG-021, "Trusted Database Management System Interpretation of The Trusted Computer System Evaluation Criteria (TCSEC)," April 1991

NCSC-TG-022, "A Guide to Understanding Trusted Recovery in Trusted Systems," December 30,1991

NCSC-TG-024, Version-1 Vol 1/4, "A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements," (this guideline)

Vol 2/4, "A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators," (draft)

Vol 3/4, "A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial," (draft)

Vol 4/4, "A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document - An Aid to Procurement Initiators and Contractors" (draft)

NCSC-TG-025, "A Guide to Understanding Data Remanence in Automated Information Systems," September 1991

NCSC-TG-026, "A Guide to Writing the Security Features User's Guide for Trusted Systems," September 1991

NCSC-TG-027, "A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems," May 1992

NCSC-TG-028, "Assessing Controlled Access Protection," 25 May 1992

NTISSAM COMPUSEC/1-87, National Telecommunications and Information Systems Security (NTISS) "Advisory Memorandum on Office Automation Security Guideline," January 16,1987

OMB Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information," July 9,1990

OMB Circular Number A-71,"Security of Federal Automated Information Systems," July 5 1978

OMB Circular Number A-109, "Major System Acquisitions," April 5,1976

OMB Circular Number A-123, "Internal Control Systems," August 8,1986

OMB Circular Number A-130, "Management of Federal Information Resources," December 12, 1985, Appendix III "Security of Federal Automated Information Systems"

OPM 5 CFR Part 930, "Training Requirements for the Computer Security Act," Interim Regulation, July 13,1988

Public Law 100-235, "Computer Security Act of 1987," January 8,1988

C.2 AGENCY/PROTECTION-SPECIFIC BIBLIOGRAPHY

In addition to the National and DoD requirements, a DoD organization is usually required to conform to one or more of the documents listed in this appendix. These documents are derived from the National-level documents, but provide more detail and interpretation as to how specific National-level requirements are to be met in specific arenas. Other documents in this list deal with the protection of a specific type of information sensitivity. This guideline addresses only the National and DOD level guidance and does not, in general, delve into the more specific guidance provided by documents in this list.

Air Force Regulation 205-16, "Automated Data Processing Systems Security Policy, Procedures, and Responsibilities," April 28,1989

Air Force Special Security Memorandum (AFSSM) 5024, "Computer Security in Acquisitions," 12 November 1991

Army Regulation 380-19," Information Systems Security," August 1,1990

Brooks Act of 1965 (Public Law 89-306), (Title 40, United States Code, Section 759) "Automatic Data Processing Equipment"

Director of Central Intelligence Directive 1/1 6, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)," (SECRET), July 19,1988

DIA, "Security Manual for the Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," Supplement to Director of Central Intelligence Directive

DIAM 50-3, "Physical Security Standards for Sensitive Compartmented Information Facilities," May 2,1980

DIAM 50-4, "Security of Compartmented Computer Operations (U)," (CONFIDENTIAL), June 24,1980

DIAM 50-5 VI, "Sensitive Compartmented Information"

Department of Energy Order 5635.1A, "Control of Classified Documents and Information," February 12,1988

Department of Energy Order 5637.1, "Classified Computer Security Program," January 29, 1988

DoD Directive 5100.36," Defense Scientific and Technical Information Program"

DoD Directive 5200.5, "Communications Security (COMSEC)," April 21,1990

DoD Directive 5200.19, "Control of Compromising Emanations," February 23,1990

DoD Directive 0-5205.7, "Special Access Program (SAP) Policy," January 4,1989

DoD Directive 5210.2, "Critical Nuclear Weapons Design Information," January 12, 1991

DoD Instruction C-5210.21, "Implementation of NATO Security Procedure (U)" (CONFIDENTIAL)

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31,1984

DoD 5230.25-PH, "Control of Unclassified Technical Data with Military or Space Application," May 1985

DoD Directive 5400.7, "DoD Freedom of Information Act," May 13,1988

DoD Directive 5400.11, "Department of Defense Privacy Program," June 9,1982
FIPS PUB 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," U.S. Department of Commerce, NBS (now NIST)

JCS Staff Memorandum 313-83, "Safeguarding the Single Integrated Operational Plan (SIOP)"

Marine Corps Order P5510.143, "Marine Corps Automatic Data (ADP) Security Manual"

NACSIM 5203, "Guidelines for Facility Design and Red/Black Installations (U)," (CONFIDENTIAL/NOFORN)

National Telecommunications and Information System Security Instruction No 7000, "TEMPEST Countermeasures for Facilities," October 17,1988

NCSC 2, "National Policy on Release of Communications Security Information to U.S. Contractors and other Non-Governmental Sources," National Communications Security Committee Publication

Nunn-Warner Amendment (Title 10, United States Code, Section 2315), "Law Inapplicable to the Procurement of Automatic Data Processing Equipment and Services for Certain Defense Purposes"

Office of the Chief of Naval Operations (OPNAV) Instruction 5239.1A "Department of the Nary Automatic Data Processing Security Program, March 8, 1982

Title 5, United States Code, Section 551, "Administrative Procedures Act"

Title 35, United States Code, Section 181-188, "Patent Secrecy"

Title 18, United States Code, Section 1905, "Disclosure of Confidential Information Generally"

Ware, W. H., ed., "Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security," AD-A076617/0, Rand Corporation, February 1990, reissued October 1979