Defense Information Systems Agency
Center for Standards

DEPARTMENT OF DEFENSE TECHNICAL ARCHITECTURE FRAMEWORK FOR INFORMATION MANAGEMENT

Volume 5:
Program Manager's Guide for Open Systems

Version 3.0

30 April 1996

This page intentionally left blank.

FOREWORD:
ABOUT THIS DOCUMENT

This edition of the Technical Architecture Framework for Information Management (TAFIM) replaces Version 2.0, dated 30 June 1994. Version 3.0 comprises eight volumes, as listed on the following configuration management page.

This is the first release of Volume 5, *Program Manager's Guide for Open Systems*. This document release is intended to generate comments and feedback from the Department of Defense (DoD) information management (IM) community.

TAFIM HARMONIZATION AND ALIGNMENT

This TAFIM version is the result of a review and comment coordination period that began with the release of the 30 September 1995 Version 3.0 Draft. During this coordination period, a number of extremely significant activities were initiated by DoD. As a result, the version of the TAFIM that was valid at the beginning of the coordination period is now "out of step" with the direction and preliminary outcomes of these DoD activities. Work on a complete TAFIM update is underway to reflect the policy, guidance, and recommendations coming from theses activities as they near completion. Each TAFIM volume will be released as it is updated. Specifically, the next TAFIM release will fully reflect decisions stemming from the following:

- The DoD 5000 Series of acquisition policy and procedure documents
- The Joint Technical Architecture (JTA), currently a preliminary draft document under review.
- The C4ISR Integrated Task Force (ITF) recommendations on Operational, Systems, and Technical architectures.

SUMMARY OF EXPECTED UPDATES

Volume 5 is still a prototype document in many respects. Authors and subject matter experts are currently reworking several sections to address both user comments and previously identified needs. Sections of the document remain incomplete due to the unavailability of information and/or time and funding. Volume 5 will, however, continue to evolve and be adjusted to reflect the IM community's need for program management guidance.

In addition to harmonization with the documents listed above, the next version of Volume 5 will reflect:

- The results of interviews currently being conducted with DoD C4I and information systems program managers

- Review comments and feedback on this version of the document received from the IM community

- The coordinated definitions being developed by DISA/D5 in the draft document *Information Systems Architecture Relationships and Definitions* that is being staffed separately.

A NOTE ON VERSION NUMBERING

A version numbering scheme approved by the Architecture Methodology Working Group (AMWG) will control the version numbers applied to all future editions of TAFIM volumes. Version numbers will be applied and incremented as follows:

- This edition of the TAFIM is the official Version 3.0.

- From this point forward, single volumes will be updated and republished as needed. The second digit in the version number will be incremented each time (e.g., Volume 7 Version 3.1). The new version number will be applied only to the volume(s) that are updated at that time. There is no limit to the number of times the second digit can be changed to account for new editions of particular volumes.

- On an infrequent basis (e.g., every two years or more), the entire TAFIM set will be republished at once. Only when all volumes are released simultaneously will the first digit in the version number be changed. The next complete version will be designated Version 4.0.

- TAFIM volumes bearing a two-digit version number (e.g., Version 3.0, 3.1, etc.) without the DRAFT designation are final, official versions of the TAFIM. Only the TAFIM program manager can change the two-digit version number on a volume.

- A third digit can be added to the version number as needed to control working drafts, proposed volumes, internal review drafts, and other unofficial releases. The sponsoring organization can append and change this digit as desired.

Certain TAFIM volumes developed for purposes outside the TAFIM may appear under a different title and with a different version number from those specified in the configuration management page. These editions are not official releases of TAFIM volumes.

DISTRIBUTION

Version 3.0 is available for download from the Defense Information Systems Agency (DISA) Information Technology Standards Information (ITSI) bulletin board system (BBS). Users are welcome to add the TAFIM files to individual organizations' BBSs or file servers to facilitate wider availability.

This final release of Version 3.0 will be made available on the World Wide Web (WWW) shortly after hard-copy publication. DISA is also investigating other electronic distribution approaches to facilitate access to the TAFIM and to enhance its usability.

TAFIM Document Configuration Management Page

The latest **authorized versions of the TAFIM** volumes are as follows:

Volume 1: Overview	3.0	30 April 1996
Volume 2: Technical Reference Model	3.0	30 April 1996
Volume 3: Architecture Concepts & Design Guidance	3.0	30 April 1996
Volume 4: DoD SBA Planning Guide	3.0	30 April 1996
Volume 5: Program Manager's Guide for Open Systems	3.0	30 April 1996
Volume 6: DoD Goal Security Architecture	3.0	30 April 1996
Volume 7: Adopted Information Technology Standards	3.0	30 April 1996
Volume 8: HCI Style Guide	3.0	30 April 1996

Other working drafts may have been released by volume sponsors for internal coordination purposes. It is not necessary for the general reader to obtain and incorporate these unofficial, working drafts.

Note: Only those versions listed above as authorized versions represent official editions of the TAFIM.

CONTENTS

APPENDICES

FIGURES

This page intentionally left blank.

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this volume of the Technical Architecture Framework for Information Management (TAFIM) is to provide program managers and their supporting Government and contractor staffs with guidance for developing technical architectures in planning and managing command, control, communications, computers, and intelligence (C4I), and information systems programs, either migration or new acquisition programs. Volume 5 is a guide for applying and integrating the principles and guidelines of the TAFIM and other Department of Defense (DoD) guidance documents promoting an open systems environment (OSE) for information systems. The information provided in this volume is intended to assist C4I and information systems program managers in making sound management decisions that result in OSE-compliant systems.

1.2 SCOPE

Volume 5 contains guidance for those C4I and information systems program management areas where OSE principles and standards should be incorporated in planning and management. This guidance applies to all DoD Components in the management of new C4I and information systems, the modernization of existing C4I and information systems, and the upgrade of existing C4I and information systems components under the direction of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I). This includes all C4I and information systems programs, projects, activities, and information systems (including migration systems) that are to be acquired and managed in accordance with the DoD 8000 series directives and are subject to the TAFIM.

Volume 5 is currently in its first version; however, it encompasses and supports the information contained in the most recent issues of the other TAFIM volumes. As the TAFIM and new and existing C4I and information systems policies and directives emerge and evolve, Volume 5, following the approval and publication of this version, will also evolve to reflect the latest guidelines and resources available.

1.2.1 Intended Audiences and Uses

Volume 5 has several intended audiences. The primary audience consists of the chartered C4I and information systems program managers within the DoD Components. Additional audiences comprise other DoD C4I and information systems managers and their staffs, to include support contractors, involved in TAFIM-related activities. The use of Volume 5 is essentially the same for all audiences — to provide insight into the TAFIM and help locate required information concerning a variety of functional and technical topics related to C4I and information systems architectures and OSE. The volume also points to the other TAFIM volumes and additional DoD information sources that will provide more in-depth explanation and assistance on a selected subject area. All publications cited as references can be found in Appendix C.

1.3 BACKGROUND

An information system includes support and mission-oriented applications, computing platforms, and communications networks. The current DoD information system technical infrastructure consists largely of stovepipe, single-purpose, and inflexible systems that are costly to maintain. These systems reflect a multiplicity of approaches to migrate toward open systems, with each system progressing along its own path with limited attention to interoperability.

The evolving DoD enterprise vision for information management (IM) emphasizes integration, interoperability, flexibility, and efficiency through the development of a common, multipurpose, standards-based technical infrastructure. This vision requires a new paradigm for building technical architectures and information systems that improve the effectiveness of functional operations and promote efficient use of technology throughout the DoD. In support of the DoD IM vision and goal, the TAFIM provides the single DoD technical architecture framework for managing multiple technical architecture initiatives and also provides the prescribed guidance and basis for evolving the DoD's technical architecture toward the DoD OSE initiative. Its use is directed in the series of DoD memoranda identified in Section 1.4 that mandate the TAFIM for this purpose.

The TAFIM consists of a cornerstone set of documents, including this document, which provide sound guidance for ensuring improved user productivity, development efficiency, portability, scalability, interoperability, and system security, while promoting vendor independence and reduced life-cycle costs. Currently, the TAFIM includes the following eight volumes:

- **Volume 1 - Overview.** Provides an overview of the TAFIM.
- **Volume 2 - Technical Reference Model (TRM).** Provides the conceptual model for information services and their interfaces.
- **Volume 3 - Architecture Concepts and Design Guidance.** Provides concepts and guidance to support the development of technical architectures.
- **Volume 4 - DoD Standards-Based Architecture Planning Guide.** Provides a standards-based architecture planning methodology.
- **Volume 5 - Program Manager's Guide for Open Systems.** Provides guidance to ensure that the principles and objectives of open systems are used in developing technical architectures and in planning and managing C4I and information systems programs.
- **Volume 6 - DoD Goal Security Architecture.** Addresses security requirements commonly found within DoD organizations' missions.

- **Volume 7 - Adopted Information Technology Standards (AITS).** Provides the DoD profile of standards and guidance in terms of TRM services and interfaces.

- **Volume 8 - Human Computer Interface (HCI) Style Guide.** Provides a common framework for HCI design and implementation.

The TAFIM embodies effective, flexible interoperability and integration capabilities and helps identify and establish a uniform and cohesive architecture framework and guidance structure for the establishment of technical architectures. While the TAFIM does not provide a specific architecture, the intent is to provide the assistance, services, standards, design concepts, and configuration that can be used to guide the development of technical architectures that meet specific mission requirements. It is independent of mission-specific applications and their associated data and can be applied to all information systems technical architectures, in all DoD organizations and environments (e.g., strategic, tactical, sustaining base).

As a whole or by independent volume, the TAFIM is a valuable tool for program managers in carrying out their information technology (IT) duties and responsibilities. To assist program managers in utilizing the TAFIM and meeting its objectives, TAFIM Volume 5 has been prepared to provide guidance in those program management areas where the incorporation of TAFIM principles and guidelines will assist in meeting DoD OSE objectives.

1.4 DOD POLICY ON TAFIM APPLICATION

The following DoD memoranda mandate the TAFIM as DoD-wide, IM technical architecture guidance and address its use in systems migration, data standardization, and process improvement:

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Memorandum, “Technical Architecture Framework for Information Management (TAFIM),” 30 March 1995.

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Memorandum, “Selection of Migration System,” 12 November 1993.

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Memorandum (with attachment), “Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement,” 13 October 1993.

Appendix D contains the text of these and other pertinent policy documents addressing the use of the TAFIM.

1.5 PROPOSING CHANGES TO TAFIM DOCUMENTS

Appendix G contains the guidance and directions for submitting a proposed change to the TAFIM, including this Volume 5.

1.6 DOCUMENT OVERVIEW

Volume 5 contains four sections and nine appendices, as described in the following table.

Section	Description
1 Introduction	In addition to this document overview, Section 1 contains the purpose and scope of Volume 5; the background and purpose of the TAFIM, including relationship of Volume 5 to the other TAFIM volumes; DoD policy mandating the use of the TAFIM; and information on proposing changes to TAFIM documents.
2 Overview of Open Systems Architecture Objectives	Provides the definition of OSE and addresses OSE in relation to the evolution of the current DoD technical infrastructure and its guiding principles.
3 Areas of OSE Concern in C4I and Information Systems Program Management	Describes and addresses those elements of program management where OSE principles and standards should be incorporated into the C4I and information systems management process.
Appendix A: Acronyms	Contains a list of acronyms.
Appendix B: Definitions	Provides definitions of the terms used in Volume 5.
Appendix C: References	Contains a table of all resource documents cited in Volume 5 and their sources.
Appendix D: TAFIM Policy Memoranda	Contains the text of all policy memoranda pertaining to the TAFIM.
Appendix E: Systems Engineering Elements/Activities and Products	Contains a table describing the various elements and/or activities of Systems Engineering process discussed in Section 3.15.
Appendix F: DISA OSE Information Services	Contains a table of services available from DISA that can provide support to activities using the TAFIM.

Section	Description
Appendix G: Program Management Responsibilities Matrix	Contains a matrix of all program management activities discussed in Volume 5; the documentation to be produced in relation to each activity; and the DoD management level(s) responsible for the activities and products identified.
Appendix H: Proposing Changes to TAFIM Documents	Contains instructions for submitting TAFIM changes.
Appendix I: Information System Architecture Relationships and Definitions	Contains a definitive set of architecture components and definitions to structure the complexity of architecture related phrases used within the DoD.

This page intentionally left blank.

2.0 OVERVIEW OF OPEN SYSTEMS ARCHITECTURE OBJECTIVES

This section provides the definition of OSE and its purpose in the evolution of the current DoD technical infrastructure. The guiding principles or characteristics of an open system are also discussed in relation to their role in the design and development of OSE-compliant systems.

2.1 EVOLUTION TO OPEN SYSTEMS

The DoD technical infrastructure is evolving into an open system environment in response to a real need for information and resource sharing across differing or incompatible levels of information ownership (i.e., enterprise). As computer technology evolves, so do the practices and methodologies employed to integrate new technologies into the workplace. Included are the many principles developed for software engineering, which continue to be expanded upon and enhanced to guide/define the open systems environment.

Computer programming has evolved into software engineering in large part because of emerging requirements for software interfacing, structured programming, data sharing, distributed environments, etc. These requirements in turn have resulted in the introduction/acceptance of shared databases, relational database management systems (DBMSs), modularization (functional separation), software reuse, data standardization, standard interfaces, and the development of American National Standards Institute (ANSI), International Organization for Standardization (ISO), and Institute of Electrical and Electronics Engineers (IEEE) standards. As these requirements and practices have been applied at the system level (i.e., within a system), their intrinsic value has been recognized as applicable at the functional level (i.e., between systems). Figure 2-1 shows the relationships of systems within a functional area (arrows indicate information flow). As systems proliferate, the need for inter-system communications/integration at the functional level becomes clear. As technology advances, it becomes more and more important that each system be able to “talk” to other systems, within and outside of its own functional area. With these new requirements comes the further development of interface standards, refinement of data standards, categorization and allocation of services, etc. With the advent of networks and the introduction of open systems, more effective communication has become possible within and across functional areas, as depicted in Figure 2-2 (arrows indicate communication flow), as well as between the various levels of the Enterprise Model described in TAFIM Volume 1, Section 5.

The DoD IM Integration Model, also depicted in TAFIM Volume 1, Section 5 (Figure 5-1) shows the various interfaces across the Enterprise Model. As these possibilities for communications have emerged, so has the need for a DoD-wide open information infrastructure to support the various Services and missions of the defense community. In response to this need, the concept of the Defense Information Infrastructure (DII) has been developed.

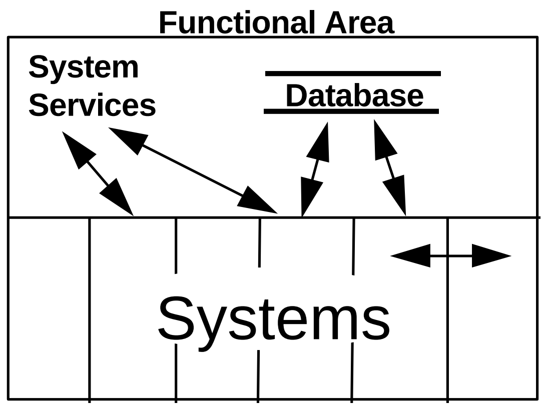

Figure 2-1. System Interfaces

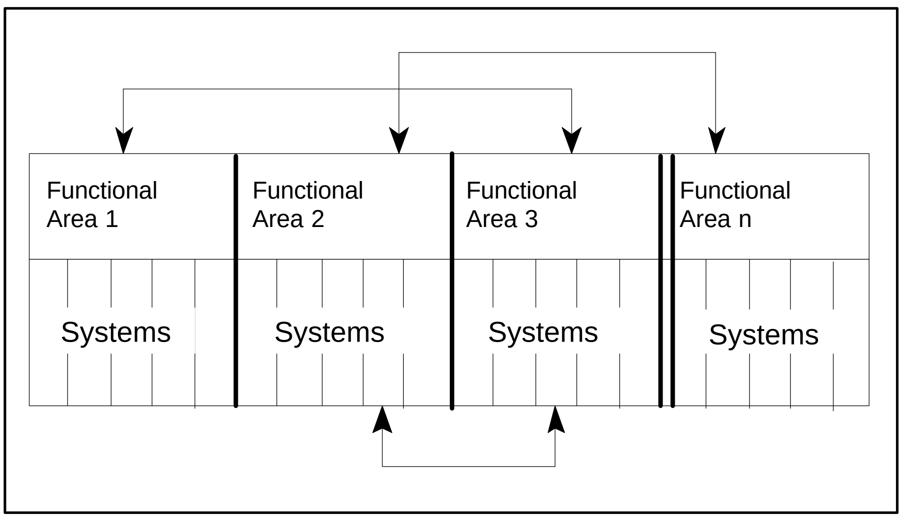

Figure 2-2. Functional Interfaces

The DII is envisioned to be a "...seamless web of communications networks, computers, software, databases, applications, data, and other capabilities that meets the information processing and transport needs of DoD users..."[1]

The goal architecture of the DII includes the Defense Information System Network (DISN); interfaces for Government, industry, and academia; satellite and other remote communications links; local, regional, and global control centers; and megacenters. The DII is an evolving infrastructure, for which the operational target date is the year 2000. A complete discussion of DII architecture, applications, and services can be found in DISA's *Defense Information Infrastructure (DII) Strategic Enterprise Architecture*.

---

[1] *Defense Information Infrastructure (DII) Strategic Enterprise Architecture*, DISA, Coordination Draft, May 31, 1995, pages 1-2.

A variety of other definitions of an open system, along with a discussion of standards and standards profiles, can be found in Section 1 of the *Next Generation Resources (NGCR) Acquisition Guide*.

2.2 GUIDING PRINCIPLES OF THE OPEN SYSTEMS ENVIRONMENT

"An Open System Environment encompasses the functionality needed to provide interoperability, portability, and scalability of computerized applications across networks of heterogeneous, multi-vendor hardware/software/communications platforms. The OSE forms an extensive framework that allows services, interfaces, protocols, and supporting data formats to be defined in terms of nonproprietary specifications that evolve through open (public) consensus-based forums." [2] Open systems with their set of applied standards are intended to function efficiently in the OSE. A well-developed and deployed OSE also supports data sharing and software reuse as well as cross-functional requirements.

The TAFIM provides the sound guidance and basis for evolving the OSE framework, which requires that the following OSE characteristics be incorporated in the engineering and design of C4I and information systems:

- **Standards-based** - importance of standardized data, interfaces, and architecture.

- **Portability** - capability to move from one environment to another through use of standardized data and interfaces, common languages, etc.

- **Scalability** - capability to move from one environment to a smaller or larger environment (including increased/decreased data flows) through use of standardized data and interfaces, common languages, etc.

- **Interoperability** - capability to communicate and operate with disparate systems within and outside of the primary operating environment through use of standardized data, interfaces, and architecture.

These characteristics are considered to be the basic "guiding principles" that program managers should take into consideration in planning and managing their programs. The program management areas where OSE principles should be of concern to the program manager are described in Section 3. The relationships of the OSE principles to the program management areas and guidance that may assist the program manager in assuring that these principles are properly addressed and incorporated in technical program activities are provided in Section 4.

---

[2] *Guide on Open System Environment (OSE) Procurement*, Gary E. Fisher, NIST Special Publication 500-220, October 1994, page iii.

This page intentionally left blank.

3.0 AREAS OF OSE CONCERN IN C4I AND INFORMATION SYSTEMS PROGRAM MANAGEMENT

Program management in the DoD can be defined as a systematic, coordinated process for selectively and collectively accomplishing the technical and managerial functions necessary to attain the timely, effective, and efficient acquisition and operation of systems and services. This section reviews the planning and implementation of program management process activities and products in which OSE principles and standards should be incorporated. The emphasis is on the program management of major system acquisitions; however, the same management principles and functions should apply to all C4I and information systems acquisitions, regardless of size. Modified management approaches and instructions unique to each Service may also apply, although the aspects of a program that must be demonstrated should be identical.

References to the DoD directives, standards, and other guidance documents, including the TAFIM, that contain complete direction and the recommended management approaches for subject area implementation are provided in each program area write-up. (Appendix C contains the complete listing of all references used.) These references should be reviewed if more in-depth information is required in a particular program management area. Also, Appendix F contains a listing of DoD services that can provide additional information or guidance in a particular subject area. A consolidated view of the program management activities discussed in this section, including the products to be produced and the management responsibility, is provided in Appendix G.

3.1 FUNCTIONAL PROCESS IMPROVEMENT

Functional process improvement (FPI) is an iterative management process by which information management in the DoD is defined and evolved. Although not formally considered a part of the life-cycle management (LCM) process, the FPI process precedes the initiation of the LCM process and eventually feeds most programs into the LCM process once system initiatives are identified and defined. FPI involves the streamlining and standardization of current processes, data, and C4I and information systems across the DoD. As depicted in Figure 3-1, FPI begins with the elimination of non-value-added activities and continues through rigorous analyses to identify changes in the way missions and functions are accomplished. It is through the FPI process that a mission need is defined or revised and C4I and information systems are developed or modified.

The Office of the Secretary of Defense Principal Staff Assistants (OSD PSA), along with the Chairman of the Joint Chiefs of Staff, has overall responsibility and authority to define DoD functional requirements and evaluate and improve current processes, data, and the supporting C4I and information systems. Direction, requirements, and guidelines for FPI are contained in DoD 8020.2-M (Draft) and 8020.2-M, Change 1, which establish the process improvement responsibilities and procedures for all DoD areas and activities. DoD 8020.1-M also provides

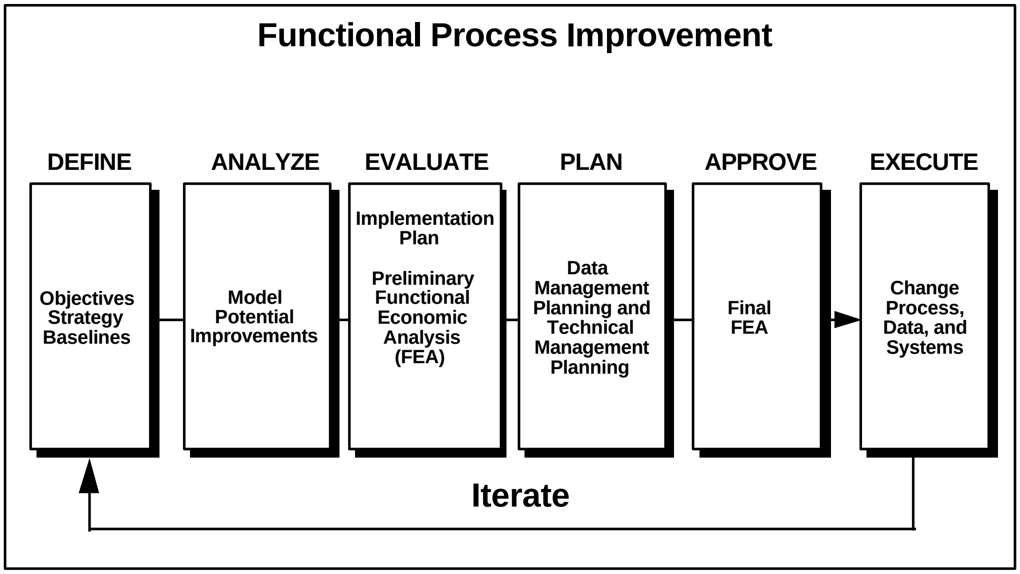

Figure 3-1. Functional Process Improvement Process

information on the services and support mechanisms available to assist in performing FPI. The services provided by the Defense Information Systems Agency (DISA) are identified in Appendix F of this document. The *Acquisition and Technology (A&T) Architecture Development Handbook (Draft)* is an additional information source identifying the relationships and links between the FPI process and the standards-based architecture (SBA) process[1] - a process that intersects with and supports the development of the FPI-required products (e.g., Corporate Information Management Implementation Plan, Functional Area Strategic Plan, Baseline Analyses, Functional Economic Analyses, Functional Architecture) produced during the FPI process. A description of the SBA process can be found in TAFIM Volume 4.

3.2 MIGRATION PLANNING

Migration planning involves assessing the functional, technical, data, and programmatic dimensions of C4I and information systems within a functional area and determining the future of those systems identified as migration systems. In this respect, the purpose of migration planning is to identify systems that best meet functional area requirements and support improvement initiatives in processes, data, and infrastructure. This includes assessing and eliminating systems where duplication of functionality exists, assessing new technology and best practices, selecting standard systems (i.e., migration systems), conducting a detailed assessment of supporting infrastructures, developing acquisition and integration strategy, developing an implementation strategy, and developing and deploying the systems. Products of migration planning may include Integration Decision Papers and Technical Integration Plans, influenced by Functional Economic Analyses (FEA) developed during the FPI process (see Section 3.1), and migration strategies and plans.

[1] The SBA Process guides the application of the technical architecture framework and provides a standard methodology for the development of technical architectures.

A more precise description of migration planning, including the requirements and responsibilities for this activity, are contained in DoD 8020.2-M (Draft) and DoD 8020.2-M, Change 1. TAFIM Volume 4, *DoD Standards-Based Architecture Planning Guide*, also provides a methodology for planning and implementing system migration as part of the SBA process. The SBA process depicted in the guide is an effective means of performing migration planning activities and can assist an organization in advancing selected migration systems toward the target architecture of all selected systems identified for the organization and feeding service requirements to the DII.

3.3 REQUIREMENTS

The requirements engineering phase of the life-cycle is recognized as one of the most important phases. Decisions made during this phase can have a significant impact on design, its implementation, integration, and testing. Program managers must be aware of the importance of this phase and the relationships among the different types of requirements and their impact on the program and system baselines. An understanding of these relationships, or the lack thereof, can have a significant impact on the cost and schedule of any program.

Depending on need and schedule, an acquisition or development manager can build a system in isolation (i.e., unfettered by policy or directives). More traditionally, the program manager considers the DoD policies, directives, acquisition guides, etc., when developing the system. A third scenario brings in all the former requirements and, in addition, takes into consideration adjunct requirements. The emergence of adjunct requirements (i.e., requirements that are levied on a program and are external to the system's set of performance requirements) can present added constraints or demand additional resources in the development process. Typically, adjunct requirements are not fully understood, defined, or considered in the conceptual or early life-cycle phases. Their impact will become evident in the development phase and more significant during implementation. Systems can be developed in the absence of adjunct requirements and still meet the intended set of operational and performance requirements; however, their inclusion in a development can represent significantly added scope.

An increasing demand for systems deployment in complex operational scenarios containing cross-functional interfaces and requiring conformance to Open System principles results in the creation of adjunct requirements. Introducing new technologies into a development can further increase the set of adjunct requirements. Adjunct requirements also require a framework for implementation and are needed to define a complete application portability profile. Program managers will be affected by adjunct requirements if their systems are required to implement in a particular DoD mandated language (e.g., Ada); utilize reusable components (e.g., design, architecture, software); adopt certain standards or methodologies (e.g., ICAM Definition Method [IDEF], object-oriented); utilize a particular environment or tool set (e.g., Computer-Assisted Software Engineering [CASE], Integrated Computer-Assisted Manufacturing [I-CASE]); procure from a standard set of defined resources (e.g., hardware, instruction set, chip set); adopt standardized components and/or security elements (e.g., operating system, compartmented mode workstation, database); and incorporate or introduce a new technology previously excluded. The degree of impact on a program will depend on the life-cycle phase in which the adjunct requirement is introduced and on the type of resources required to implement it. Adjunct requirements generated from these activities can result in added schedule or cost, unless their impact is understood and planned for early in the life-cycle.

Policies, directives, orders, and guidelines also directly drive or influence a manager's program. They establish a direction that must be conformed to and a set of schedule milestones that DoD management will monitor. They represent higher order constraints or mandates that affect the entire life-cycle. These key policies and directives are considered as pseudo-adjunct requirements, since they are recognized and understood by program managers and are planned for as an integral part of the acquisition and development process.

Figure 3-2 shows an optimum Requirements Model including adjunct requirements (i_1 and i_2 are iterations). A traditional Requirements Model is depicted in the three central boxes of Figure 3-2. The traditional model shows user requirements driving system requirements, which in turn drive the derived and allocated requirements. These requirements, in turn, are driven (or at least affected) by policy, directives, and orders, also depicted in the figure. As a system becomes more complex and as users become more sophisticated, the need for more constraining or modulating requirements will typically arise; the Requirements Model takes on a corresponding level of complexity from the introduction of the adjunct requirements. The introduction of adjunct requirements forces the model to become more of a process, in which the application of adjunct requirements necessitates further interaction between the requirements themselves and iterations of the process.

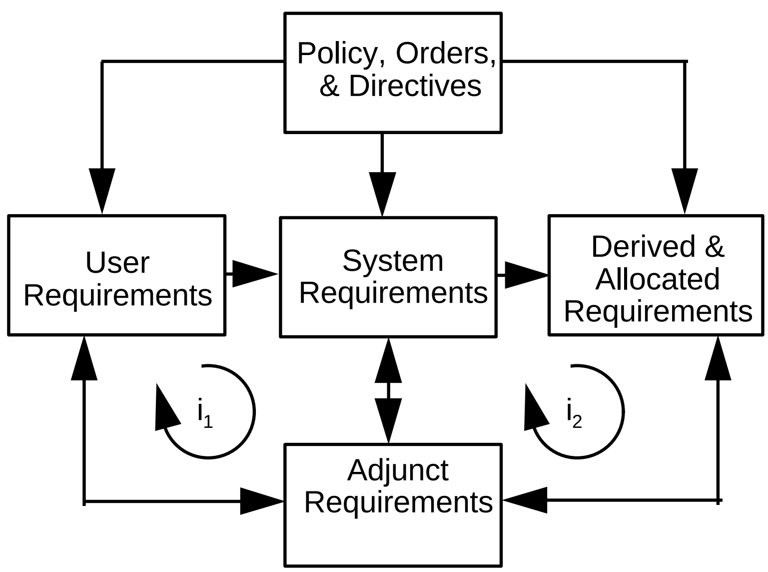

Figure 3-2. Requirements Model

The model is provided to make the program manager aware of the need to plan judiciously based on program needs and an extended set of requirements (i.e., the adjunct requirements). The model should assist in the development of a disciplined requirements process, which is necessary for the orderly translation of incomplete and informally identified user requirements into formalized, traceable system requirements.

A well-defined requirements process enables the development of appropriate requirements models to assist in this definition and refinement. Furthermore, such a requirements process will enable a separation or clear distinction between system prototypes (intended to optimize the design relative to requirements), and a requirements model (intended to define and mature system requirements). This distinction between models and prototypes will subsequently enable the synthesis of design derived directly from executable specifications in support of these prototypes and generated automatically by CASE tools or other design automation aids.

3.4 DETERMINING MISSION NEED

For C4I and information systems, mission need determination begins when the functional user identifies deficiencies or shortfalls in existing defense capabilities, identifies technological opportunity, or determines more cost-effective means of performing assigned tasks within the mission area. The functional user further defines or revises the perceived mission need through functional process review and information needs analyses, during which time alternatives to new development, use of commercial or existing systems, or tactics changes that may satisfy the existing or emerging need are considered and identified. When no other alternative is available, a Mission Need Statement (MNS) is developed to summarize the results of the analysis process and to document the mission need leading to the development of a new or modified C4I and information system. Approval of the MNS at Milestone 0 starts the life-cycle management process and establishes the program for system development or modification.

3.4.1 Mission Need Statement

The MNS defines and documents a mission need and justifies resource expenditures to identify and explore alternative solutions or system design concepts. At a minimum, the MNS describes the current organization and operational environment, with emphasis on existing functional processes, and identifies deficiencies in existing capabilities, new or changed functional requirements, and/or opportunities for improvement. It also addresses constraints and assumptions for functional, technical, and financial areas that may have an impact on potential alternative solutions; the relationships of the identified need to the current Corporate Information Management Strategic Plan[2] and Enterprise Integration (EI) Implementing Strategy[3] and functional area strategic planning and direction; the system location and general schedule for the implementation and deployment of the new or modified functionality; and any

---

[2] *Corporate Information Management for the 21st Century, A DoD Strategic Plan*, ASD/ C3I, June 1994

[3] *DoD Enterprise Integration (EI) Implementation Strategy*, DISA Center for Integration and Interoperability, June 1994

cooperative opportunities, such as a program addressing a similar need at another DoD or federal organization or within an allied nation.

The functional user prepares the MNS in accordance with DoD 8120.2-M, Part 2, and submits it for validation and approval in accordance with DoD 8120.2 paragraphs E.2.b, E.2.c, and E.8.e. The appropriate OSD Principal Staff Assistant and the Chairman of the Joint Chiefs of Staff, or a designated representative, validate the initial MNS, depending on the acquisition category of the program (i.e., major versus nonmajor system). The appropriate Milestone Decision Authority (MDA) approves the validated MNS at Milestone 0. The complete MNS may be updated, if appropriate, and revalidated for each milestone review subsequent to Milestone 0. It is also updated, if appropriate, and revalidated at the time a C4I and information system is designated as a migration system. DoD 8120.2 and DoD 8120.2-M provide further guidance on MNS validation and approval. Additional information regarding the milestone review process is provided in Section 3.12.1.

3.5 STANDARDS AND STANDARDS PROFILES

Standards are the complete, consistent suite of guideline documentation that reflects common consent among the organizational bodies on products, practices, or operations. Their primary purpose is to control the variability of products and processes. For example, information technology standards provide technical definition for processes, procedures, practices, methods, materials, items, engineering practices, operations, services, interfaces, connectivity, interoperability, information formats, content, interchange, transfer, and other standardization topics. They are also the basis for all life-cycle decisions affecting interoperability, portability, and scalability and are essential in achieving Open Systems design.

To ensure the intended compatibility, interpretability, and integration of C4I and information systems, IT standards planning and the documentation of selected standards are mandated by the DoD 8120 series of life cycle management directives and the TAFIM. This DoD policy clearly stipulates that all C4I and information systems programs are required to accomplish standards planning, including the identification of information technology profiles, in accordance with the TRM for Information Management, previously discussed in Section 2 and fully described in TAFIM Volume 2. In this respect, each program is required to prepare and produce an IT standards profile beginning no later than Milestone I, with future updates, thereafter, in each system life cycle phase. The standards profile is required for inclusion in the System Decision Paper (SDP) submitted, by the program manager, for each milestone decision. It also accompanies the Test and Evaluation Master Plan (TEMP) at Milestones II, III, and IV for standards conformance test planning purposes.

3.5.1 Applying the TRM to Standards Profiles

A knowledge and understanding of the TRM, discussed in TAFIM Volume 2, provides the insight needed to develop and identify standards/standards profiles, support environments, migration strategies, and technology issue resolution, since the TRM is a mechanism for establishing relationships/linkages between service areas, the services themselves, and standards. Establishing these linkages provides the basis for selecting environments and their services to ensure interoperability. It also provides the basis for prioritizing tasks/acquisition components and standards as a function of the life cycle and "best time to effect." The latter is equivalent to the emerging concept of "just-in-time engineering/manufacturing" used to reduce inventories and maintenance costs.

Knowledge of the TRM, service areas and services, and the available standards identified in the AITS and ITSG mentioned above also contributes to the effective planning and implementation of acquisition strategies and program activities. By establishing relationships and mappings of standards to services and service reference models (e.g., NIST/ECMA Special Publication 500-211), a program manager can select tools in an ordered and prioritized manner, precluding a costly initial investment in those tools, that can be obviated by technology transfer rates offering increased functionality and capability in next-generation products and environments.

3.5.2 Developing Standards Profiles

A standards profile is a defined set of one or more standards, and where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards necessary for accomplishing a particular function. The standards profile may contain a set of one or more base standards, along with specific subsets, classes, options, and parameters necessary to accomplish a particular function. The specific profile becomes part of the program documentation baseline and matures with the system design as the program progresses through each life-cycle phase. The requirements specified within the profile are included in systems acquisition documentation as performance requirements, functionally allocated to, and integrated appropriately into program and contract documents, such as specifications, Statements of Work (SOWs), proposal evaluation criteria, proposal instructions and formats, and contract data requirements.

TAFIM Volume 7, *Adopted Information Technology Standards (AITS)*, provides architects and system planners with the definitive set of IT standards for standards profile development. Implementing activities are encouraged to select from this repertoire of standards to meet the needs of specific mission areas. Use of these standards will help provide a consistency across the enterprise, mission, function, and applications levels of the DoD Integration Model, as described in TAFIM Volume 1, and will enable program managers to guide their programs toward a collective DoD OSE.

A companion document to TAFIM Volume 7 to be used in the selection of standards and the development of standards profiles is the *Information Technology Standards Guidance* (ITSG). The ITSG is the foundation document for the AITS. It provides amplifying implementation guidance for those standards identified in TAFIM Volume 7 as well as supporting information on AITS standards hierarchies. The ITSG also includes information on related or emerging standards precluded from the AITS, and recommendations for specifying standards in system acquisition documentation. Because of the ever-constant changes in standards, the program manager should also monitor Government and industry trends and keep abreast of ISO, IEEE, ANSI, etc., and new developments in preparing standards profiles.

The Center for Standards, within DISA and responsible for the evolution of IT standards policy, will provide customer assistance in applying the information found in the AITS and ITSG. Users of AITS and ITSG information are encouraged to contact the Center for Standards for assistance or to identify functional requirements and/or standards not yet incorporated in these documents. (See listing for Center for Standards in Appendix F.)

3.6 DATA ADMINISTRATION, DATA MODELING, AND DATA STANDARDIZATION

Data administration is the function that oversees the management of data across all facets of an organization and is responsible for central information, planning, and control. Department of Defense Directive (DoDD) 8320.1, *DoD Data Administration*, establishes the policies for the administration of data in the DoD and authorizes a DoD Information Resource Dictionary System (IRDS) as a primary tool of data administration. As discussed in DoDD 8320.1 (Enclosure 3), the responsibilities of planning, managing, and regulating data are assigned to the DoD Data Administrator (DoD DAd), located within the DISA Center for Software (see Appendix F). The DoD DAd implements and manages DoD-level data administration policies and procedures and supports the development and management of useful, available, and accessible information to enable the successful execution of the mission of the Department. The DoD DAd also tracks all the entities and data elements that represent the emerging DoD standard information requirements and provides the technical infrastructure for data administration, including the DoD Data Model, the Defense Data Dictionary System (DDDS), and procedures for data modeling, data standardization, data security, data quality assurance, and database operations.

The DoD DAd has enacted the Defense Information Management Program, which requires that accurate and consistent information be available to decision makers for the effective execution of DoD missions. The program operates with the following objectives in mind:

- To develop the DoD Enterprise Data Model (EDM) to depict overall DoD mission needs and support operational capabilities requiring the collection, storage, and exchange of data.

- To develop data elements for standardization through data modeling efforts.

- To create a base of shared information through the DoD EDM and standard data structures and elements. This will enable functional and technical personnel to perform their tasks in an integrated, effective, and efficient manner.

- To implement data administration aggressively in ways that provide clear, concise, consistent, unambiguous, and easily accessible data DoD-wide.

- To standardize and register data elements that meet the requirements for data sharing and interoperability among C4I and information systems throughout the DoD.

- To use applicable federal, national, and international standards before creating DoD standards or using common commercial practices.

Each DoD Functional Area assigns a Functional Area Data Administrator (FDAd) to implement data administration procedures and serve as the functional area representative on functional issues affecting DoD data administration. The FDAd also identifies data administration resources needed in the Functional Area and identifies functional requirements for submission to the DoD data administrators.

Component Data Administrators (CDAd) are assigned to help implement data administration procedures across all functional areas within the Component. They identify the interface between the users, database administrators, and application developers of the C4I and information systems within the DoD Component and ensure Component adherence to DoD data administration policies, procedures, and standards.

The uniform management and operating procedures established for use by all DoD levels in managing and implementing DoD data administration activities and products are found in DoD 8320.1-M, *Data Administration Procedures*. This manual implements the data administration program established by DoDD 8320.1 and provides the mission, goals, benefits, and concept of operations of the data administration program; the roles, relationships, and responsibilities of the DoD data administration community; program management procedures for sustaining the data administration function; and procedures for maintaining and using a technical infrastructure.

3.6.1 Data Modeling and Standardization

A data model is the graphical and textual representation of data a business needs to accomplish its mission. It is a representation of data objects that can be shared and reused across application systems, organizational boundaries, and different functional areas. Models provide information about the interests of an enterprise; facilitate improvements in strategies, tactics, and operations; provide a basis for database design; facilitate an understanding of data leading to the identification of sharing possibilities; and reduce redundant data entry and unintentional replication of data. The basic steps of DoD data model development include data model reviews by data administrators at all DoD levels to ensure data standardization, which promotes data sharing, software reuse, and, most importantly, interoperability. These reviews ensure the proposed entities, attributes, and relationships identified in the data model adhere to mandatory technical and functional requirements and are representative of the DoD-wide data standardization perspective provided in the DoD EDM.

The DoD EDM is the integrated view of the data requirements of the functional areas and Components in the DoD. It is developed and continuously extended based on reviews of data models developed to document data requirements across DoD functional areas. It is also the infrastructure to support the DoD data administration objectives. DoD C4I and information systems that are to conform to DoD data administration procedures are to be developed in this DoD-wide perspective, through the use of modeling tools and standard metadata. The manual, *DoD Enterprise*

Data Model Development, Approval, and Maintenance Procedures (DoD 8320.1-M-x), is interim guidance for developing data standards that are to become part of the EDM. This manual should be used in conjunction with DoD 8320.1-M-1, *Data Element Standardization Procedures*, in the development, approval, and maintenance of EDM-related products.

DoD 8020.1-M (with Change 1), *Interim Management Guidance on Functional Process Improvement*, provides additional guidance on data modeling, while TAFIM Volume 4 (and its associated *A&T Architecture Development Handbook [Draft]*) provides methods for identifying opportunities for data improvement, when exploring business improvement opportunities. A process for developing data requirements and shared information approaches can also be found in Section 4 of the working draft of the *Acquisition and Technology (A&T) Corporate Information Management/Enterprise Integration (CIM/EI) Program Management Structure*.[4] A wide array of information on data modeling and standardization is also available from the DISA Center for Software (see listing of services in Appendix F), responsible for the promulgation of the aforementioned policy on data standardization and modeling and the maintenance of the EDM. The Center for Software also operates and maintains the DDDS discussed in the following subsection.

3.6.2 Defense Data Dictionary System

The Defense Data Dictionary System (DDDS) is a centrally controlled, DoD data repository put in place and managed by the DoD DAd to receive, store, support access to, and manage standard data definitions, data formats, usage, and structures (e.g., architectures, subject area models, and other data model products). Specifically, the DDDS is to assist the DoD in creating and maintaining a repository system in the following ways:

- Collect and store standard elements and their attributes
- Identify DoD organizations and processes using standard elements as defined in information models
- Provide convenient, on-line data element documentation query and reporting capabilities throughout the DoD
- Provide the capability to track the state of each standard element throughout its life-cycle, from its proposed candidacy through its archival and deletion
- Provide the capability to identify the impact of proposed changes on standard elements.

The DISA Center for Software should be contacted for further information and guidance on DDDS services (see Appendix F).

[4] Provides a framework and uniform management structure for implementing the CIM/EI program within the A&T community.

3.7 ESTABLISHING ARCHITECTURES FOR OPEN SYSTEMS

An Open Systems architecture depicts a system in which the components, both hardware and software, are specified in an open manner. In establishing an open system architecture, the Program Management Office (PMO) must determine the needs and functional requirements to be fulfilled by the system through the in-depth analysis of:

- **Target system requirements** - including data, communications, hardware, security, applications, etc.

- **Existing infrastructure**- including wide area networks (WANs), local area networks (LANs), servers, routers, communications, applications, etc.

These analyses are then used to identify integration needs and evaluate integration issues. The program manager must be cognizant of all developments above the program level (i.e., enterprise, mission, or functional area level) in regard to the open architecture, as it is a “living” and “dynamic” entity. The functional requirements must also be applied across the various open hardware and software standards to meet the system requirements. The use of open standards allow product choices with compatible interfaces that can be combined to create an open system architecture. The use of standards and common functional and technical architectures contributes to standard, portable, scalable, and interoperable systems for which individual components can be acquired and configured, by different executive agents, over an extended period of time. Within the umbrella of common architectures, data, applications, and infrastructures can be managed according to their separate life-cycles and integrated into complete systems.

There are a variety of architecture models to choose from in the establishment of functional and technical architectures for C4I and information systems. Each has its advantages and disadvantages, and each must be evaluated in light of the system requirements and environment (i.e., open, legacy, or migration). Components may be mixed and matched from the various architecture models, as long as services are allocated per the Technical Reference Model and as long as a standards profile is adhered to. Architecture concepts and design guidance for use in establishing an architecture are contained in Section 3 of TAFIM Volume 3. The preferred methodology for planning and implementing an architecture is presented in TAFIM Volume 4, *DoD Standards-Based Architecture Planning Guide*. DISA’s *Architecture Relationships and Definitions* should be used in order to become familiar with the basic architecture concepts. Also, a close association with DISA should help ensure that the program is on track with recent developments.

3.8 SYSTEM SECURITY

In each C4I and information systems endeavor, program management and staff must consider security at all levels and throughout the system life-cycle to provide multifaceted, cost-effective protection of the data being processed or transmitted. A security program with basic principles and safeguards that assure data confidentiality, reliability, accuracy, and availability, and that maintains accountability for actions within the operational environment should be fundamental to the design, implementation, operation, and maintenance of the system. This concept allows for confidentiality that limits data access to individuals with a need to know; reliability that data are not altered and results are accurate; availability that assures data are on hand when needed; and accountability that audits activities for responsibility of accomplishment.

The inclusion of information systems security throughout the planning and development process provides for cost-effective fielding of systems that are legal and regulatory-compliant. Accordingly, legal and regulatory guidelines have evolved to govern Federal Agency and Department information security operations. These guidelines range from Public Law 100-235, the Computer Security Act of 1987 and its implementation instruction (Office of Management and Budget [OMB] Circular 90-08), to National Computer Security Center (NCSC) directions, the “rainbow series”, and Departmental regulations (i.e., DoDD 5200.28, DoD 5200.28-M, DoD-Standard (STD)-5200.28-STD, DoDD 5200.5, DoD 5200.1-R, and DoD 8120.2-M), which require the preparation of a System Security Policy and System Security Plan for milestone decision review.

Conformance to Open System requirements also adds a layer of complexity to security concerns. In an Open System, secure data are potentially accessible to more users than in a closed system. Special attention should be paid to emerging protocols, multilevel security schema, etc. Although the specification and application of security standards does not totally ensure a secure system or design, the program manager must be sure that security engineering is performed with the most current standards in mind and in accordance with the DoD Goal Security Architecture (DGSA), a primary consideration in establishing a security structure for C4I and information systems. The DGSA is an evolving, generic security architecture, developed by the DISA Center for Information System Security (CISS), under the Defense Information Systems Security Program (DISSP), a joint undertaking of DISA and the National Security Agency (NSA). TAFIM Volume 6 addresses the security requirements of the DGSA and the process by which organizations can identify the specific security requirements of their missions. In brief, the DGSA specifies the security principles, concepts, functions, and services that target security capabilities to guide system architects in developing their specific architectures. It also includes a generic security architecture that provides an initial allocation of security services and functions. Program managers should become familiar with the DGSA, as described in TAFIM Volume 6, and with the other applicable security guidance mentioned above, to assure legal and regulatory compliance with DoD and federal security guidelines and initiatives.

The Center for Systems Engineering within DISA is responsible for the development of TAFIM Volume 6 and can be of assistance in providing additional information and guidance on the DGSA. The Center for Systems Engineering is listed as a resource in Appendix F.

3.9 ESTABLISHING THE PROGRAM MANAGEMENT TEAM

The key to a successful program is to establish a management structure that reflects the mission of the organization yet remains flexible enough to accommodate the needs of the program. The organization and management of the program should also be consistent with the importance and scope of the program. To comply with the C4I and information systems LCM policy and guidance in the DoD 8120 series of directives, a C4I and information systems program manager must be assigned at the beginning of the LCM Phase 0, Concept Exploration and Definition, in time to explore alternative system design concepts. The program manager is selected based on the level of education, training, experience, and other qualifications required of program managers, as specified in DoD 5000.52.M, *Career Development Program for DoD Personnel Manual*. The program manager ideally is a multidisciplined, experienced manager with sufficient tenure and interest in the program to provide continuity and establish accountability for program actions. The individual should be capable of establishing a program structure and program work force that compliments project size and technical complexity and should be knowledgeable about and capable of managing the programmatic and technical elements identified in the program structure.

The program manager should also be aware of the current topics of emphasis found in congressional testimony, DoD policy statements and speeches, and in the media, since some of these topics attain permanence by being incorporated into DoD directives or instructions. Most important, in managing the design and development of an Open System, the program manager must understand the functional and technical architecture framework in which the assigned system will perform and must be willing to enforce standard practices in all management and technical processes.

3.9.1 Program Management Charter

Program objectives are developed that set forth the capability in terms of mission need, cost, and schedule goals being sought by DoD upper-level managers when establishing the requirement for new or modified C4I and information systems. These objectives are communicated to the program manager by the DoD management authority (i.e., Deputy Secretary of Defense, or designated authority, etc.) in a written charter that serves as a contract between the program manager and the chartering authority. In addition to program objectives, the program manager's charter defines the authority, organization, resources, responsibility, scope, and methods of operation of the C4I and information systems program, as well as the lines of authority and accountability. The charter is prepared and processed in accordance with the policy, instructions, and procedures contained, respectively, in DoDD 8120.1, Department of Defense Instruction (DoDI) 8120.2, and DoD 8120.2-M.

3.9.2 Program Management Team

A responsibility of the program manager is to recruit a staff or identify a program management team with the requisite skills and experience to manage the assigned system. In putting together a team for an Open Systems project, the personnel requirements for the team should be determined based on the work identified in the contract, specifically in the SOW and in the Contract Data Requirements List (CDRL) discussed in Section 3.14. The Work Breakdown Structure (WBS), discussed in Section 3.13 and linked directly to the SOW, is also a source for determining team skill requirements, since it defines the work to be accomplished and assigns resources and responsibilities to the work elements identified. Resource requirements may also be determined from the results of market and trade studies discussed in Section 3.11.

The most critical work elements in accomplishing OSE objectives are the technical engineering management organizations established within a program. These organizations, individually or as a whole, are the program manager's front line with the user. The effectiveness of these organizations depends on how well they are institutionalized in the program and how cognizant and sensitive they are to Open Systems issues and TRM service areas and views pertaining to architecture and standards. The leadership and control implications of these program elements are driven by the program size, program maturity (life-cycle phase), number of system segments, interface complexity, and individual skills. A generic technical engineering management structure for a development and integration type effort, however, is typically organized under the guise of systems engineering management. This organization may include all or some of the following types of personnel, with all or a mixture of the skills described:

- **Systems manager (chief engineer).** Lead technical manager who controls the architecture and all project-level engineering plans. Also manages the project's technical baseline and speaks for the program manager on technical issues. Has leadership skills, communication skills, a generalist perspective; pays attention to detail; and has a broad project experience in the areas of engineering, development, and test. Should report directly to the program manager.

- **Systems architect.** Plays a subordinate role to the systems manager and is responsible for the "vision" of the system, as stated in user requirements and desired expectations. Guides the development process from "cradle to grave." Is a participant in requirements development; is responsible for high-level systems design; and guides the design and test process. Has a sense of vision, communication skills, and the ability to work at the abstract level.

- **Systems engineer.** Plans, manages, and monitors all systems engineering activities. Develops and maintains systems functional, developmental, and operational "test-to" requirements. Analyzes requirements and allocates to system design. Identifies and allocates derived requirements within specialty engineering domains. Has leadership skills and broad engineering experience, with an ability to pay attention to detail. Should report directly to the systems manager or systems architect.

- **Systems test manager.** Plans/monitors all verification activities and is responsible for system integration and requirements compliance verification, including configuration item acceptance testing, item-to-item integration and checkout, system-level test (including external interface test), and system regression testing. Has systems engineering experience, communication skills, development experience; and pays attention to detail. Should report directly to the program manager.

- **Quality assurance manager.** Is the program manager's independent review authority. Ensures that project processes are being followed, including the management of project metrics, and audits for requirements compliance. Has standards and policy awareness, considerable systems engineering skills and experience; is process-centered with continuous improvement awareness; and has a broad project perspective. Should report directly to the program manager.

- **Configuration management (CM) manager.** Determines and coordinates all CM activities, including configuration control board activities; determines and monitors contractual CM requirements; establishes relationships with interfacing CM organizations;

and ensures continuity and that uniform CM practices and procedures are followed. Like the quality assurance manager, is aware of standards and policy; has considerable systems engineering skills and experience; is process-centered with continuous improvement awareness; and has a broad project perspective. Should report directly to the program manager.

- **Systems engineering personnel.** Perform/monitor requirements analysis, system design, and system test planning functions during the initial phases of the project. Possible transition to verification and operational support tasks (testing, tech manuals, installation, and checkout, etc.) following approval of the critical design. Should report to the systems manager or systems architect.

- **Engineering specialty engineers.** Specialty engineering includes domains that require detailed expertise beyond the scope of the typical engineer or developer and including those engineering disciplines that influence system design, development, and operational support of a product, such as reliability and maintainability engineering, performance engineering, risk management, human factors engineering, safety engineering, life-cycle cost analysis, and logistics engineering. Specialty engineers with specific expertise are typically integrated into a program to:

  - Analyze and recommend engineering specialty requirements
  - Tailor standards and specifications to meet specialty requirements
  - Develop contract SOW input, specification input, and deliverable requirements
  - Evaluate offerers' responses
  - Prepare detailed specialty engineering management plans
  - Review development contractors' deliverables
  - Evaluate contractors' progress/conformance at design reviews
  - Monitor tests and conduct specialty tests
  - Evaluate operational performance
  - Evaluate engineering change proposals (ECPs).

Each engineering specialty should be part of the systems engineering organization during the initial phases of a program but may spin off or migrate from the systems engineering domain to become its own entity as development progresses.

3.10 DETERMINING PROGRAM STRATEGY

The program strategy is a combination of business and technical management concepts designed to achieve program objectives within imposed resource constraints. It is the method utilized to project design, development, and deployment requirements for the C4I and information systems and is the basis for formulating the acquisition plan and subsequent functional program plans, which guide the C4I and information systems program throughout its life-cycle.

The program manager formulates the program strategy during the concept exploration and definition phase of the LCM process and incorporates it in the Program Management Plan (PMP) for approval at the Milestone I review. DoDI 8120.2 identifies and describes four program strategies that may be considered: grand design, incremental, evolutionary, and other. The PMP preparation guidelines provided in DoD 8120.2-M identify the specific requirements for documenting the chosen strategy.

Government and contractor objectives should be clearly stated in the program strategy, as should the level of competition, estimate of contract value, type of contract, time phasing, and program incentives. It is also the program manager's responsibility, by means of the program strategy, to remain consistent with basic LCM policy but to tailor the LCM phases, activities, and milestones (see Section 3.12) to best fit the unique requirements and conditions of the program. In this regard and depending on the selected strategy, the program strategy may recommend combined or repeated milestone decision points, as well as associated activities within a life-cycle phase, if required. The number of replicated decision points, as well as the manner in which the increments between decision points will be reviewed, is included in the initial program strategy at Milestone I. The program strategy may be updated or refined in the subsequent life-cycle phases; however, any modification must be approved by the MDA.

Program strategy should be refined by requirements for interoperability, scalability, and especially, portability. Some other considerations in formulating the program strategy may include the general OMB policy to rely on the private sector for proposing solutions to functional requirements and to use contracting as a tool in the acquisition process (see OBM Circular A-109), and other necessary considerations, which include the favorable and unfavorable lessons learned from similar programs; recognition of and accommodations for risks and uncertainties; the proper relationship of risk sharing between the Government and the contractor; the Government tailoring of specifications and standards in consonance with contractor efforts (the objective being to avoid nonessential constraints on contractors); the optimal use of Government laboratories in furnishing technical direction during system development; the use of Non-Developmental Items (NDI)/Commercial-off-the-Shelf (COTS) products in lieu of development; and the possible reuse of existing resources. Section 1 of the *Next Generation Computer Resources (NGCR) Acquisition Guide* provides a detailed discussion of the advantages and disadvantages of a program strategy that includes NDI acquisition.

3.11 EXPLORING ALTERNATIVES THROUGH MARKET ANALYSIS

Selecting the right products for an Open System Environment requires conducting a market analysis based on market surveys, technical risk analysis, supportability risk analysis, mitigation techniques, and life-cycle cost impact assessments. Information derived from market analysis becomes an economic driver for possibly reviewing (possibly revising) requirements, as well as planning, budgeting, and implementing system upgrades and support. The remainder of this section addresses market surveys, trade studies, and trade-off analyses, which are decision-making tools that can be used in determining and evaluating the current technology market and OSE product options.

Market surveys provide the rationale for make or buy decisions and provide information on technologies, existing products, market share commercial production practices, and industrial capabilities. The results of market surveys are incorporated into the requirements decomposition process and used in technology assessments.

Two types of market surveys are typically performed: the initial market survey and the market investigation. During the initial market survey, defined system requirements should be compared with features of OSE-compliant products. The objective of this survey is to establish an awareness of the marketplace and to determine what products are available as NDI. One of the most important first steps in conducting the initial survey is early communication of the requirements to the vendors identified (OEMs, their representatives, and their suppliers). Such information includes operating parameters for hardware and software, environmental constraints, interface and integration requirements, etc., that will allow each vendor to better answer questions about possible solutions to the requirements. The subsequent market investigation is conducted following the identification of potential product sources, as obtained in the initial market survey, to obtain more specific information on the product and source so that a final decision can be made.

Other types of evaluation open to a program manager in making program decisions are trade studies and trade-off analyses. Trade studies are performed typically by the contractor throughout development as an essential part of the systems engineering process. Trade studies are controlled by systems engineering to integrate and balance all design-for and engineering specialty requirements and to compare candidate hardware and software standards and products available to meet program needs. As a formal decision analysis method, trade studies are used to solve any complex problem that has more than one selection criterion and to provide documented decision rationale for review by a higher authority. These analyses are necessary for establishing system configurations and for accomplishing detailed design of individual components. The trade study method is equally applicable to budgeting, source selection, test planning, logistics development, production control, and design synthesis. Trade-off analysis also provides a structured analytical framework for evaluating a set of alternative concepts or designs. Trade-off analysis is typically used in source selection, but it can also be used when criteria for study or parameters are conducive to objective evaluation or amenable to a numerical performance measurement scheme.

Additional information on market analysis, specifically information on how to conduct market research and surveys, can be found in Section 6 of the DISA *Acquisition How To Guide*.

3.12 LIFE-CYCLE MANAGEMENT PROCESS

The system life-cycle consists of the interval from system inception through system disposal. All activity in the system life-cycle centers on the state of definition of the system configuration at any time in its life-cycle. The Department of Defense uses a systematic technical management process to control the system life-cycle, as promulgated in accordance with the DoDD 8120.1, *Life-Cycle*

Management (LCM) of Automated Information Systems, DoDI 8120.2 *Automated Information System Life-Cycle Management Process, Review, and Milestone Approval Procedures*, and DoD 8120.2-M, *Automated Information System Life-Cycle Management Manual*. As depicted in the directives, the process includes five life-cycle phases (Concept Studies Decision; Concept Exploration and Definition; Demonstration and Validation; Development; Production and Deployment; and Operations and Support), with sets of phased activities and periodic reviews, including milestone decision reviews at Milestone 0, I, II, III, and IV. Each milestone review is conducted by the appropriate MDA, discussed in Section 3.12.1, to determine how well program requirements are being met and risks are being managed. The DoD Component acquisition executives, program executive officers (PEO), and program managers are charged with the responsibility of the programs under their control to provide the focus and management to develop, field, and support the programs to meet user needs. These managers must work closely with their various counterparts in the Office of the Secretary of Defense and the appropriate committees to ensure the program is ready to proceed from one life-cycle phase to the next.

The required program management activities to be accomplished in each LCM phase, including the essential program documentation required for milestone decision, are identified in the DoD 8120 series of directives mentioned earlier. The program documentation listed in DoD 8120.2-M, which provides the core procedures and content requirements for milestone decision documentation, are the primary means for conveying to the MDA a complete description of the program activities and program issues. The documentation is intended to reflect the accomplishment and/or current status of specific planning and analysis tasks to be conducted before each milestone review, and is a synthesis of the existing program plans and essential information prepared by the various program organizations to support and guide the system acquisition. Also, the systems engineering documentation identified in Section 6 of DoDI 5000.2 may be developed and submitted as appendices to the PMP, should program activities and complexity warrant the development of such documentation. The PMP and other program documentation required by DoD 8120.2-M, as well as the planning documents that may be required from DoDI 5000.2, Section 6, are depicted in the Program Management Responsibilities Matrix contained in Appendix G.

3.12.1 Milestone Decision Authorities and Reviews

Periodic, formal program reviews (either scheduled milestone decision reviews or in-process reviews) are required before a C4I and information systems program can advance from one LCM phase to the next. The purpose of each review is to give management a current status of the program and to allow management to provide additional guidance and/or give milestone approval for advancement to the next life-cycle phase.

The MDA is responsible for conducting the milestone review and is assigned based on the acquisition category of the C4I and information systems program (major verses nonmajor) as described in DoDD 8120.1. For major C4I and information systems programs falling outside the purview of the Under Secretary of Defense for Acquisition (USD[A]), the MDA is ASD (C3I), who is the DoD senior IM Official designated in accordance with DoD Directive 5137.1. This authority may be re-delegated to the lead acquisition authority, DoD Component head, DoD Component acquisition executive, or the Senior IM official within the DoD Component. For nonmajor C4I and information systems programs, the DoD Component head is the designated MDA. This authority may also be further delegated to the appropriate lowest level, commensurate with the resources and risk involved.

The MDA performs formal program reviews in accordance with the LCM policy, responsibilities, process, and procedures of DoD 8120.1 and DoD 8120.2, and the uniform procedures for conducting LCM activities and preparing LCM documentation in DoD 8120.2-M. For non-major C4I and information systems programs, the MDA adheres to the various LCM policies and procedures established by the respective DoD Component heads and the OSD PSAs. Through the review and analysis of the LCM documentation required for MDA review, the designated MDA provides the C4I and information systems program manager and staff with the appropriate program direction. Milestone approval, conditional milestone approval, or approval of specified activities must be obtained before program management may proceed with activities in the next life-cycle phase. A review is successfully completed when the MDA makes management judgments on what program activities may be permitted and specifically authorizes those activities for next life-cycle phase implementation

3.12.1.1 The Defense Acquisition Board

The Defense Acquisition Board (DAB) is the oversight management mechanism for major Defense acquisition programs. It is the primary forum used by the DoD Components to resolve issues, provide and obtain guidance, and make recommendations to the Under Secretary of Defense for Acquisition on matters pertaining to the DoD acquisition system. Formal DAB reviews are conducted at each milestone to assess Service accomplishment of the previous phase and to assess readiness to proceed to the next phase of the LCM process. The USD(A) may also hold special in-process reviews between milestones, when warranted.

The USD(A), as the Defense Acquisition Executive (DAE), chairs all program and milestone decision reviews for major defense acquisition programs (DoDD 5000.1/DoDI 5000.2). To help the DAE conduct milestone reviews, four DAB committees (Strategic Systems, Conventional Systems, C3I Programs, and Major Automated Information Systems) have been established. These committees conduct pre-DAB reviews and develop, investigate, and resolve program issues.

3.12.1.2 The DoD Major Automated Information System Review Council

The DoD Major Automated Information System Review Council (MAISRC) is the life-cycle management review body for all major C4I and information systems subject to review under the policies and procedures of the DoD 8000 series Directives. It is composed of a chairperson, members, an Executive Secretary, and staff. ASD (C3I) chairs and operates the MAISRC (independently of the DAB) in resolving program issues and facilitating milestone decisions in the role of MDA. The MAISRC conducts milestone reviews to evaluate the completion of the minimum required LCM accomplishments and exit criteria; provides advice on program readiness to the MDA and recommends appropriate movement to the next LCM phase; determines the adequacy of proposed plans for subsequent LCM phases; and recommends exit criteria for each milestone review. (DoDI 8120.2 and DoD 8120.2-M should be reviewed for further details on this process, including the documentation required and specific responsibilities of the program manager and other review participants. Appendix G, however, does identify the overall MAISRC documentation required for each milestone review in accordance with DoD 8120.2-M.)

3.12.1.3 The In-Process Review

The MDA may call an in-process review (IPR) at any time within the life-cycle of a program to determine current program status, progress since last milestone review, program risk and risk-reduction measures, and potential program problems that require guidance. An IPR will also be called when there is a breach in the program baseline. As requested by the MDA, the program manager will be required to submit documentation for MDA review. The documentation is assembled from existing program management documentation and may be supplemented with additional documentation required to support specific issues to be addressed at the IPR.

3.12.2 The System Decision Paper

The System Decision Paper (SDP) is the principle document for recording the essential C4I and information systems information critical to the DoD decision-making process, such as mission need, alternatives, management approach, schedule, resources, issues, risks, security issues, and supporting rational and decisions. The SDP represents the functional and C4I and information systems program management coordinated position for the C4I and information systems and is the primary document supporting MAISRC process. The program manager prepares the initial SDP after Milestone I, with updated SDPs submitted thereafter for each subsequent milestone review. The SDP must be approved by the appropriate level at the completion of each LCM phase in order for the respective milestone to be achieved. Part 4, Attachment 1, of DoD 8120.2-M provides the procedures and the recommended format for preparing an SDP.

3.12.3 The System Decision Memorandum

The System Decision Memorandum (SDM) documents the milestone approval decision of the MDA, the guidance provided, and the exit criteria established for the next LCM phase, including the activities to be accomplished. The MDA prepares and signs the SDM following each milestone decision review.

3.13 PROGRAM PLANNING AND CONTROL

Planning establishes the framework upon which the program manager authorizes and issues work to the task organizations. Planning is evolutionary and continues through the life of the program. The planning process breaks the WBS requirements down into subordinate elements of work appropriate to the size of the program, schedules its accomplishment, establishes budgets, and allocates resources. The work authorization process is the means by which the program manager controls the flow of work, authorizes task organizations to perform the work, and establishes performance, budget, and schedule parameters. Planning the work also requires the definition of the technical effort and the requirements for labor, material, tooling, equipment, facilities, and funding.

In addition to the WBS, the acquisition strategy, PMP, and the requirements of the Request for Proposal (RFP), SOW, specifications, and other contractual documents provide the initial impetus for planning and organizing the total program. The work effort and requirements derived from these documents culminate in the development of the WBS and other management and planning documents such as the Work Package, the Program Master Schedule, associated authorization documents, and internal Government and contractually required functional plans, such as the Systems Engineering Management Plan (SEMP), Integrated Logistics Support Plan (ILSP), TEMP, SDP, Configuration Management Plan, etc., which lay out the details for the establishment and implementation of specific segments of the overall program effort.

The remainder of this section discusses the WBS and Program Master Schedule, two of the most important tools of the program manager, and the cost/schedule and control methods used in measuring program performance.

3.13.1 The Work Breakdown Structure

A Work Breakdown Structure (WBS) is a product-oriented family tree, composed of hardware, software, services, and data that completely defines a program. The WBS displays and defines the product(s) to be developed and/or produced and relates the elements of work to be accomplished to the end product. The WBS is the foundation for:

- Program and technical planning
- Cost estimating
- Schedule definition
- Statements of work and specification of contract line items
- Progress status reporting and problem analysis.

The WBS is essential in providing the capability for the program management office to exercise technical, schedule, and financial control of the program. It also serves as the framework for the contractor's overall management system.

Four basic types of WBS formats are identified in Military (MIL)-STD-881, the standard for the WBS, although other specialized WBS that suit particular applications during design and development may be used. The four basic WBS types prescribed by MIL-STD-881 are:

- Summary WBS
- Project summary WBS
- Contract WBS
- Project WBS.

3.13.1.1 Summary WBS

A summary WBS is a structure in which the upper three levels of the WBS are specified by MIL-STD-881. The structure has a uniform element terminology, definition, and placement in the family-tree order. Appendices A through G of MIL-STD-881 provide a three-level WBS for each of the seven types of material items procured by the DoD (i.e., aircraft systems, electronic systems, missile systems, ordinance systems, ship systems, space systems, and surface vehicle systems).

3.13.1.2 Project Summary WBS

A project summary WBS is derived from MIL-STD-881 but is tailored to the specific program. This WBS is also specified to three levels of detail. The project/program office builds the project summary WBS by selecting applicable elements from the example project summary WBS in MIL-STD-881. This is usually done at the beginning of concept exploration and definition phase (Phase 0) and is included in the RFP and finalized at contract award. From this WBS, the contractor can develop individual contract WBSs (see paragraph 3.13.1.3) in compliance with the instructions contained in the RFP. (A preliminary WBS is normally part of the contractor's proposal.) The RFP contract line items (CLINs), configuration items (CIs), SOW tasks, and contract specifications, are elements of the preliminary contractor WBS. A final contractor WBS will be incorporated in the Phase 0 contract. The detail of the final contractor WBS should be extended as the program progresses in each phase, to facilitate in-house planning and control.

3.13.1.3 Contract WBS

The contract WBS is the complete WBS applicable to a particular contract or procurement action. It will generally contain the applicable portion of the project summary WBS plus any additional levels of detail necessary for planning and control. The contract WBS outlines program tasks and establishes their relation to the program organization, configuration items, and objectives. It establishes a logical indenture level for correlating performance, technical objectives, schedule, and cost, and ensures that all derivative plans contribute directly to program objectives. It also forms the basis for applying cost and schedule controls, correlating and tracing the contractor WBS to the system requirements, and defining common interfaces between specialty engineering efforts (e.g., technical performance measurement, risk management, logistics engineering, etc.) and programmatic activities (program planning, cost/schedule management, engineering management, etc.). It also plays a key role in ensuring correlation and traceability of WBS product elements.

3.13.1.4 Project WBS

The project WBS is the complete WBS for the program. It contains all WBS elements related to the development and/or production of a Defense item and is formed by combining all the contractor WBSs in a program. The project WBS may be delineated to five or six levels of detail, with the contractor responsible for developing the lower levels identified.

3.13.2 Schedule Planning

Schedule planning involves the preparation of program schedules and includes the development of the program master schedule (PMS) and subordinate schedules, based on the WBS, to ensure that all elements of the contract requirements, including hardware, software, and support items, are delivered on time. Schedules are necessary to integrate the activities of the task organizations to significant milestones.

Schedule planning should commence once the program strategy is confirmed, and requires an understanding of the current project/program dependencies at the time of development. Dependencies include those between engineering activities, those on external activities/organizations, and those by external activities/organizations on engineering products, which may be identified and tracked via either manual or automated techniques, ranging from simple charts to sophisticated activity networks used in PMS production.

3.13.3 Cost and Schedule Control

Cost and schedule control, as described in DoDI 7000.2, *Performance Measurement for Selected Acquisitions*, has two essential objectives that will benefit a major C4I and information systems program. They are: 1) the contractor shall use an effective internal cost and schedule management control system; and 2) the timely and auditable data that the Government can rely on shall be produced by the contractor cost and schedule control system.

The criteria in DoDI 7000.2 ensure that the contractor's management control systems will include policies, procedures, and methods that are designed to provide guidance to the contractor in the areas of organization, planning and budgeting, accounting, analysis and revisions, and access to data. Accordingly, a good management control system includes the following features:

- Measurement of actual work, by the contractor, through "earned value" (i.e., quantifying the amount of planned work that has been accomplished).

- Establishment and control of a program baseline, which represents the contractual schedules and is the cumulative total of all work packages within the contract. Performance is measured against this time-phased budget plan.

- Breakdown of performance measurement by product, through the use of the WBS (i.e., the WBS should completely define the entire program and provide summary levels for performance reporting).

- Breakdown of performance information by organization or function. The cost account is formed at the intersection of the WBS and the contractor's organizational structure. The WBS and functional organization is integrated by identifying the organizations responsible for performing specific tasks.

- Summarizing and reporting of progress information in a disciplined manner. The criteria provides specific formats and data elements that the Government will use to monitor contractor performance, validate contractor status reports, and seek out trends that might affect the program in a positive or negative manner.

- Conduct of variance analysis to identify variances in performance at the cost account level, and corrective action.

3.13.3.1 Cost and Schedule Performance Reporting

Two reports can be generated for the collection of summary contractor performance data. They are: 1) the cost performance report (CPR) and 2) the cost/schedule status report (C/SSR). The reports provide the program manager with contractual information regarding cost, schedule, and technical performance. Both reports are described in DoDI 7000.10, *Contract Cost Performance, Funds Status, and Cost/Schedule Status Reports*. The CPR is used generally to obtain performance data in conjunction with the application of cost/schedule control system criteria (C/SCSC) to a fixed-price incentive or cost-reimbursable contract that meets specified dollar thresholds for research and development or procurement. The C/SSR is intended for the application to contracts more than 12 months in duration where application of the CPR is inappropriate.

The Government can order summary performance data from the contractor's internal control system by placing the requirement for the CPR or C/SSR in the contract (in the SOW and CDRL). In addition to providing an effective channel of communication between the contractor and the Government, the additional benefits of obtaining these data include reporting objective performance status, cost impact of known problems, capability to trace problems to their source (organizational and WBS), and quantification of schedule deviation in dollars from the contract plan.

3.13.3.2 Cost/Schedule Control System

Although many tools on the market, from mainframes to personal computers (PCs), are used for effective program management, no single set of management control systems will meet every contract management data need for performance measurement. Because of variations in organizations, products, and working relationships, it is not feasible to prescribe a universal system for cost and schedule control; however, any system used by the contractor should meet the criteria described in DoDI 7000.2.

The responsibility for developing and applying the specific procedures for complying with the criteria is vested in the contractor. The contractor is required to provide performance data directly from the same system used for internal management control. The basic purpose is to assure that the contractor has in place, and uses, adequate cost and schedule control systems and provides reliable contract status at least monthly.

An element in the evaluation of proposals should be the contractor's system for planning and controlling contract performance. Although DoDI 7000.2 criteria does not require the use of specific systems, the contractor should be contractually required to submit to the program office the CPR and/or C/SSR, at a minimum, on a network system or floppy disk, in a structured American Standard Code for Information Interchange (ASCII) format. The program may in turn use these data to support the many tools available to streamline and automate the analysis and reporting processes associated with analyzing the contractor's reports.

3.14 CONTRACT MANAGEMENT/SOURCE DETERMINATION

The many functions of contract management/source determination are performed by various organizations and individuals, both internal and external to the project/program management office, in the contracting process. This section focuses on those functions and products of the process where the guiding principles for OSE development should be incorporated into the contracting activities and products.

3.14.1 The Request for Proposal

Program managers generally use the competitive proposal method of procurement, in which the RFP is the solicitation instrument. The RFP is a formal, official communication between Government and industry in the contracting process. It describes the Government's needs for goods or services and is the vehicle for soliciting proposals from industry to fulfill those needs. It also provides the frame of reference for source selection, contract definition, and management reviews.

The clarity and coherence with which the RFP is constructed can favorably or unfavorably affect the events to follow. How clearly the Government communicates its need in the RFP, for instance, will almost certainly influence the quality of proposals received, the ease or difficulty in conducting source selection and negotiation, and ultimately, the success or failure of contract performance.

The Federal Acquisition Regulation (FAR) in most cases requires that contracting officers prepare written solicitations and resulting contracts using the uniform contract format outlined in the FAR. The uniform contract format is designed to facilitate preparation of the solicitation and includes Sections A through M, as follows:

- **Section A - Solicitation/Contract Form.** Cover Sheet/Standard Form 33, which contains basic information such as the issuing office address and contract number.
- **Section B - Supplies/Services/Prices/Costs.** Brief description of each contract deliverable (item, quantity, etc.), each covered by a contract line item number. Prices are entered subsequent to solicitation.
- **Section C - Description/Specifications/Work Statement.** Actual tasks to be accomplished in performance of the contract and associated specifications, including the Statement of Work.
- **Section D - Packaging and Marking.** Special packaging and marking requirements such as preservation, protection, and bar coding.
- **Section E - Inspection and Acceptance.** Place of inspection, who will inspect, and acceptance criteria.

- **Section F - Deliveries or Performance.** The time, place, and method of delivery or performance.

- **Section G - Contract Administration Data.** Accounting and paying office information.

- **Section H - Special Contract Requirements.** Requirements unique to the program and the contract (i.e., design to cost, warranties, options, Government-furnished equipment, and incentives).

- **Section I - Contract Clauses.** Commonly referred to as boilerplate and not to be overlooked. Include standard clauses of considerable power defining rights and responsibilities of contracting parties.

- **Section J - List of Attachments.** All attached forms and specifications are listed here, including the CDRL.

- **Section K - Representations, Certifications.** Any special representations required of offerors, such as small/disadvantaged business status, or Equal Employment Opportunity (EEO) compliance.

- **Section L - Instructions, Conditions, Notices to Offerors.** How to organize proposal (volume, page limits, etc.), type of contract contemplated, where to obtain copies of documents, marking of proprietary information.

- **Section M - Evaluation Factors for Award.** How the Government intends to evaluate proposals. These factors are the same as in the Source Selection Plan (SSP), which must be approved before RFP release. Typical factors or evaluation criteria include schedule, management, technical approach, and support.

The principles of OSE and the objectives of the TRM discussed in TAFIM Volume 2 apply across the board in the development of solicitations and are of particular concern in defining the requirements contained in the Statement of Work (Section C). TRM objectives should be understood and the following questions considered in the preparation of the RFP and in source selection:

- Have you specified open standards in your RFP and SOW?

- Have you defined what is expected in conformance and interoperability testing?

- Have you specified a reuse paradigm, reuse repositories, etc.?

- Does the bidder understand Open System issues?

- Is the proposal TAFIM-compliant?

- Has the bidder responded with specific open standards references?

Also, references to Portable Operating System Interface (POSIX) and Federal Information Processing Standard (FIPS) 151-2 should be included in the RFP and SOW as well as requirements specifying adherence to HCI guidelines in order to ensure user portability. (See TAFIM Volume 8, *DoD HCI Style Guide* and use as a reference.) The *Next Generation Computer Resources (NGCR) Acquisition Guide* is a resource that provides guidance and the appropriate wording for inserting Open Systems criteria and requirements into the RFP and SOW.

3.14.2 The Statement of Work

The Statement of Work (SOW) is a mandated requirement of the FAR and is developed by functional managers in the DoD in accordance with MIL-Handbook (HDBK)-245. The SOW is an essential part of the RFP and the heart of the system or equipment procurement. It is also the document by which all nonspecification requirements for contractor efforts are established and defined, either directly or with the use of specifically cited documents. The SOW expresses work efforts as minimal needs and defines those work tasks that cannot be contained in a specification (and must never be included in the CDRL or Data Item Description [DID]); however, it may be supported by specifications or may be used as a supplement to a specification.

The SOW and its associated WBS are the primary instruments upon which contractual costs are based. After the contractor has been selected and the contract awarded, the SOW becomes the standard for measuring the contractor’s effectiveness and the basis for change control. As the effort progresses, the Government and contractor refer to the SOW to determine their rights and obligations with regard to contractor responsiveness.

There are five types of SOWs defined for use in MIL-HDBK-245. Four are associated with phases of the life-cycle process. The fifth, for services, is independent of Defense material procurement phases.

3.14.2.1 Type I SOW

This SOW is usually restricted to an expression of goals and objectives when there is a limited ability to accurately identify and define a desired product. Work involving the definition and identification of alternative system design concepts (or a study effort) is usually captured in this SOW type, as are specifications, since typical programs do not have system specifications at this stage of the process.

3.14.2.2 Type II SOW

This SOW type is more descriptive of contractual work efforts and more conclusive in identifying goals and objectives. It is used to refine and define, to a lower level, the details of systems requirements, (development, manufacturing, verification, deployment, operations support, training, and disposal). The Type II SOW is, however, limited in scope to efforts required to proof or prototype, assess results of proofing and prototyping, and define system requirements to the end-item level.

3.14.2.3 Type III SOW

The Type III SOW contains enough detail to enable bidders to translate the program requirements into an effective system SEMP. It also delineates specific tasks for evolving the system requirements and technical objectives into specific system specifications (Type A), which formulate a functional baseline. The Type III SOW is prepared when a specification is used to define the quantitative and qualitative technical requirements for development, manufacturing, verification, deployment, operations support, training, and disposal. Statement of Work tasking would include all those involving the full-scale development and documentation of the intended system.

3.14.2.4 Type IV SOW

This SOW is used to culminate end efforts of the development phases by supporting production and ultimate deployment of the system. Typical tasks include producing and deploying the system per specifications and approved engineering changes, providing interim support, performing sustaining engineering and configuration management, and developing and delivering logistics support.

3.14.2.5 Type V SOW

The Type V SOW is used when the need for contractor support is identified independent of the actual development and procurement of the C4I and information systems. (Please refer to MIL-HDBK-245 for more detailed information and guidelines regarding the SOW types and SOW preparation.)

3.14.3 Selection of Standards and Specifications

Every DoD program has a set of unique specifications that define its specific technical requirements. These documents incorporate or refer to many Government standards to define items, approaches, or procedures that may be used in the development and production process. These Government standards are employed to give new programs the benefit of previous technical experience, to promote interchangeability and commonality, and to minimize costs of ownership. Implementation must be carefully considered to ensure that general standards/specifications represent current technology, yet do not create unnecessary costs to the program.

3.14.3.1 Specification and Standards Categories

Specifications are documents prepared to support acquisitions and to describe items that vary greatly in complexity. Specifications form the skeleton around which the Defense LCM process is built and are necessary to satisfy the primary objective of any procurement action. Specifications will establish the requirements in terms of both design detail and performance. There are two basic categories of specifications: general specifications, and program peculiar specifications. General specifications, referred to as military specifications, are controlled by the Defense Standardization and Specification Program (DSSP) and apply to all acquisition programs. These specifications represent a particular requirement at a particular time that can be used over and over again on many different programs. They include specifications for materials, parts, and processes; test criteria documentation; and management specifications.

Program peculiar specifications apply only to those products developed to meet specific operational requirements. The basic forms and types of these specifications are defined in MIL-STD-490A and include the system/segment specification, development specification, product specification, process specification, and material specification. As described in Section 3.5, standards are documents that establish engineering and technical requirements for processes, procedures, practices, and methods that have been adopted unilaterally.

The order of precedence for specifications and standards is (highest to lowest): Specifications (Federal, military, program peculiar); Standards (federal, military, industry); and Handbooks (Governmental). Procedures and policy for the DoD Standardization and Specification Program are promulgated by DoDD 4120.3. Specifications, standards, handbooks, and other engineering documentation prepared under DSSP are intended to state only the actual needs of the Government in a manner that will encourage maximum competition. The objectives of the DSSP are contained in DoD 4120.3-M, *Defense Standardization and Specification Program Policies, Procedures, and Instructions,* of August 1978.

3.14.3.2 Specification and Standard Selection

Government and industry are jointly responsible for ensuring that each specification and standard imposed on a contract is suitably tailored and current. The AITS in TAFIM Volume 7 should be used in selecting specifications and standards, as well as the ITSG discussed in Section 3.5. The ITSG provides amplifying implementation guidance for those standards identified in TAFIM Volume 7 and supporting information on AITS standards hierarchies.

3.14.3.3 Streamlining and Tailoring Methods

The objective of streamlining and tailoring is to clearly communicate what is required in functional performance-oriented terms at the beginning of development, and to allow flexibility for the application of the contractor’s experience and judgment. Once specifications and standards have been selected for a program, it is necessary to review and tailor the requirements contained in each specification and standard before RFP release, as well as at each milestone in the program life-cycle, if necessary. There are a number of ways to tailor specifications and procurement standards. For example, the application of a standard may be limited to specified components, or types of components, within the system by specifying the limits in the body of the system specification. Applicable portions of a standard may also be extracted for incorporation into the text of a development specification. In either case, a referenced standard may be supplemented by descriptive text in the specification to clarify the intended requirements or application. Inapplicable portions of the standard may be deleted by identifying them in an appendix to either specification.

The following are rules of thumb for specification and standards tailoring:

- At Milestone 0, specify system-level requirements in mission performance terms. Before full-scale development, military specifications and standards should be cited for guidance only.

- For development contracts, contractual applicability of specifications, standards, and related documents should be limited to those cited in the contract, and to specified portions of documents directly referenced by those cited (first-tier references). All other referenced documents (second-tier and below) should be for guidance only, unless specifically called out in the contract.

- For production contracts, those specifications, standards, and referenced documents comprising the baseline for production should be considered contractual requirements for procurement and re-procurement purposes. Acquisition streamlining should continue throughout the production phase, with emphasis on ensuring that only essential production and data requirements are carried forward into follow-on production contracts.

- When a decision is made to use COTS/NDI, all specifications and standards that define the product/items should be contractually specified in the solicitation.

- During the design process, the contractor should be required by contract to recommend detailed specifications, standards, and requirements to be applied as the system evolves toward the end product. For instance, as the system design evolves through Phase I, lower-tier specifications and standards should be selected and tailored for the next phase. Also, identified requirements should be reviewed by systems engineering; tailored, as appropriate; and identified as requirements in the development proposal. During development, a primary task should be to review and scrub lower-tier references to ensure that those specifications and standards are cost-effective. The program manager should make the final determination as to which data requirements statements, specifications, and standards should apply in production (Phase III) and throughout the remainder of the program.

Additional guidance on streamlining and tailoring is included in DoDD 5000.43 and DoD-HDBK-248, which specifies the use of contractor's management systems, internal procedures, data formats, etc., unless the program office determines that these do not meet program needs. This increased emphasis on contractor systems, procedures, and documentation increases the contractor's flexibility in generating program documentation in the most efficient and effective manner. DoDD 5000.43 further specifies procedures regarding the contractual referencing aspects of the streamlining initiative, which calls for practical measures to preclude untimely, untailored, and accidentally referenced application of military specifications and standards; that is, to specify required results rather than detailed how-to procedures in RFPs and contracts.

3.14.4 The Contract Data Requirements List

The CDRL (DD Form 1423) is the mechanism for ordering and delivering recorded information, regardless of medium or characteristics, of any nature, including administrative, financial, and technical. Several rules govern the contractual acquisition of data. Data must be set forth in a contract in a very specific way if the contract is more than $25,000. (Data requirements may be specified in the specifications/SOW if the overall contract is estimated to be less than $25,000.) With the exception of data specifically required by the FAR or Defense Federal Acquisition Regulations (DFARS), or specifically exempted by the DFARS, all deliverable data must be listed in the CDRL. The CDRL provides a single place in the contract for directing the contractor to prepare and deliver data and to meet specific approval and acceptance criteria. It establishes data required, delivery characteristics, the degree of tailoring to be applied to the DID, the points for inspection and acceptance, any interim approval requirements, and the price of the data, by DID.

Data format and content are established by data acquisition documents (usually DIDs), which, with the exception of one-time DIDs, are approved and given OMB clearance by the Defense Quality and Standardization Office. DIDs (DD Form 1664) define the data required for delivery by the contractor, including content and preparation instructions, format, intended use, and other source documents that may be used to describe the data to be delivered.

DoD 5000.19-L, *Acquisition Management Systems and Data Requirements List (AMSDL)* lists all the data acquisition documents (with the exception of one-time DIDs) that are approved and given OMB clearance in accordance with Part IX, Section B, of DoDI 5000.2. Part I of the AMSDL lists source documents and related DIDs by data functional area assignment. Part II is a numerical listing; Part III lists DIDs by key word; and Part IV lists canceled and superseded source documents and DIDs.

The DISA *Acquisition How-To Guide* (Chapter 9, "Explanation of Forms"), accessible through the DISA Library, is an excellent source for obtaining additional information on DID selection and CDRL development.

3.14.5 Source Selection Procedures

The primary objectives of the source selection process are to: (1) select contractors who can best meet Government needs as described in the solicitation/RFP; and (2) ensure that the source selection process provides for the impartial, equitable, and comprehensive evaluation of each offeror's proposal and minimizes the cost of the selection process to the Government and industry. The source selection process is managed by a three-level organization or team composed of the Source Selection Authority (SSA), the Source Selection Advisory Council (SSAC), and the Source Selection Evaluation Board (SSEB). The procedures for source selection are contained in the SSP, which the program manager prepares. The remainder of this section addresses the roles and responsibilities of the source selection team and the purpose and content of the SSP. Additional information on source selection can be found in the FAR, Subpart 15.6, "Source Selection"; DoD Instruction 5000.2, Part 10, Section B; Air Force Regulation (AFR) 70-15, "Proposal Evaluation and Source Selection"; Army Regulation (AR) 715-6, "Proposal Evaluation and Source Selection"; and Secretary of the Navy Instruction (SECNAVINST) 4200.33, "Selection of Contractual Sources for Major Defense Systems."

3.14.5.1 Source Selection Authority

The Source Selection Authority (SSA) is the Service Secretary/Component head for major systems, responsible for the overall source selection activity, but authority may be delegated to the next level. Responsibility includes approval of the Source Selection Plan, establishing the membership of the SSAC, and making the final selection decision. The SSA also ensures the evaluation criteria are consistent with the solicitation and policy.

3.14.5.2 Source Selection Advisory Council

The Source Selection Advisory Council (SSAC) is a group of senior military and/or civilian personnel representing various functional and technical disciplines. The SSAC is responsible for appointing the membership of the SSEB, establishing and applying the evaluation criteria and the numerical weighting (scoring scheme) for these criteria. The SSAC also reviews the SSEB findings, prepares an analysis of each offeror's proposal, and compares the proposals to one another. The SSAC, unless a performance risk assessment group is employed, is the body that considers contractor past performance. The output of the SSAC is a final report to the SSA on SSAC evaluations.

3.14.5.3 Source Selection Evaluation Board

The SSEB is composed of military and/or civilian personnel representing a variety of functional and technical disciplines and is assigned by the SSAC to evaluate proposals and provide narrative findings to the SSAC for use in its review. The leadership of the SSEB should be of importance to the program manager, since the staffing would consist of a cross-section of expertise from within and outside the organization, which typically includes personnel from logistics, cost analysis, operational, contract, legal, and technical areas.

3.14.5.4 The Source Selection Plan

The Source Selection Plan (SSP) establishes procedures for accomplishing the above-mentioned prime objectives. Before a solicitation is issued, the SSA approves the SSP. The program manager is responsible for preparing the plan and obtaining SSA approval before releasing the solicitation. The plan summarizes the overall acquisition strategy contemplated for the requirement and includes a discussion of the extent of competition expected, a description of the evaluation techniques to be used, and the schedule of significant actions required. It also describes the organization, membership, and responsibilities of the source selection team and identifies the evaluation factors and detailed evaluation procedures, which mirror section M of the RFP. The specific evaluation criteria are listed in the order of their importance and may include technical aspects, operational considerations, supportability management capabilities, and cost analysis. Past performance may be also be considered as an area or as an item. Representative examples of the items considered in each of these evaluation criteria areas include:

- **Technical**
  - Design Approach
  - Test Plan
  - Performance Criteria
  - Design Innovation

- **Operational**
  - Approach to Operational Concept
  - Maintainability
  - System Capability
- **Supportability**
  - Impact on Current Logistics Systems
  - Maintenance Concept
  - Supply Support
- **Management**
  - Integration Procedures
  - Interface Procedures
  - Schedule Adherence
  - Program Control
  - Past Performance
- **Cost**
  - Risk
  - Interface Procedures
  - Labor and Overhead Rates
  - Development Costs
  - Life-Cycle Costs
  - Cost Realism.

3.14.6 The Technical Data Package

The Technical Data Package (TDP) is a technical description of an item adequate for use in procurement. This description defines the required design configuration and assures adequacy of item performance. It consists of all available data such as plans, drawings, and associated lists, specifications, standards, models, performance requirements, quality assurance provisions, and packaging data, and may range from a single line in a contract to several hundreds or thousands of pages of documents. It does not include computer software or financial, administrative, cost or pricing, or management data, or other information incidental to contract administration.

The guiding standard for the TDP is MIL-T-31000, which prescribes the requirements for potential data elements and data management products for inclusion in the TDP. These requirements are tailored by the Government for inclusion in the CDRL of the solicitation/RFP, and may be tailored by the contractor in response to a solicitation using the guidelines of MIL-HDBK-248.

Contract provisions should ensure that contractors and subcontractors prepare and update TDPs as an integral part of their design, development, and production efforts. Technical data (and technical manuals) should be updated to reflect approved design changes to be made available concurrent with the implementation of the change. Additionally, the TDP that the contractor delivers to the Government should be representative of the product baseline and should have sufficient detail to permit duplicate fabrication by any competent commercial source without additional investment in design or development. However, experience indicates potential errors, omissions, inaccuracies, or nondisclosures in a TDP may pose cost, technical, and schedule risks if used in follow-on contracts; thus, TDP validation is necessary to mitigate this risk.

TDP validation should be a controlled process by which technical data can be certified as acceptable for intended use. The best validation method for use on a C4I and information systems program is the Functional and Physical Configuration Audit (see MIL-STD-973) of the producer's TDP to ensure the accuracy of drawings and other technical and supporting documentation against the design and in accordance with prescribed specifications and standards.

3.15 SYSTEMS ENGINEERING/TECHNICAL MANAGEMENT

In simple terms, systems engineering is both a technical process and a management process. The following definition identifies the technical side to systems engineering:

The application of scientific and engineering efforts to (a) transform an operational need into a description of system performance parameters and a system configuration through the use of an iterative process of definition, synthesis, analysis, design, test, and evaluation; (b) integrate related technical parameters and ensure compatibility of all physical, functional, and program interfaces in a manner that optimizes the total system definition and design; (c) integrate reliability, maintainability, safety, survivability, human engineering, and other such factors into the total engineering effort to meet cost, schedule, supportability, and technical performance objectives.

Another popular definition favors the management approach and defines systems engineering as:

The management function which controls the total system development effort for the purpose of achieving an optimum balance of all system elements. It is a process which transforms an operational need into a description of system parameters and integrates those parameters to optimize the overall system effectiveness.

With respect to each of these definitions, both the technical and management aspects of systems engineering should be applied throughout the system life-cycle to produce a successful operational system. In the planning stages of the system life-cycle, systems engineering is essential in conceiving the system concept, establishing architectures, and defining known and implied user requirements. As the detailed design is being done, systems engineers assure a balanced influence of all required design specialties, resolve interface problems, conduct design reviews, perform trade-off analyses, and assist in verifying system performance. During the development phase, concern is with verifying requirements compliance and system capability, maintaining the system baseline, and forming an analytical framework for producibility analysis. During system operations and support, systems engineering evaluates proposed changes to the system, establishes change effectiveness, and facilitates the incorporation of change modifications and updates.

The major technical tasks and the primary application of the systems engineering process are accomplished by the contractor. The quality of effort by the contractor is largely dependent on a well-defined contract that defines the Government/industry agreement with respect to the system under consideration (see Section 3.14). The RFP sets forth the systems engineering needs; the SOW provides the formal statement of those needs as requirements for the contractor; the "specification" defines the technical system requirements; and the CDRL identifies data deliverable requirements.

3.15.1 The Systems Engineering Process

Although programs differ in underlying requirements, the systems engineering process offers a consistent, logical process for accomplishing system design tasks. The process itself leads to a well-defined, completely documented, and optimally balanced system with a complete set of documentation tailored to the needs of a specific program.   Figure 3-3 illustrates the interactive activities of a basic systems engineering process. This process may be iterative and recurring during each life-cycle phase and whenever a change is initiated or needed to provide the progressive definition of the system, subsystem, and configuration items, and their verification. The level of detail involved should be commensurate with the contractual objectives of the program.

The major elements of systems engineering, including the activities and outputs of the systems engineering process, are summarized in Appendix E.

3.16 SOFTWARE ACQUISITION MANAGEMENT

Software acquisition management is the process of acquiring software, managing its development, and ensuring its supportability for the entire life-cycle. Software acquisition management activities include planning, contracting, budgeting, evaluating performance, and providing for future support of the system, as well as acquiring software, usually by contract, from a third party. Typically, the three organizations involved in the process include the customer or user of the system, the contracting agency or buyer, and the developer or seller. Depending on the scope of the effort, there may possibly be many agencies and contractors involved. While software engineering concentrates on building the software, project management focuses on managing the engineering development or acquisition.

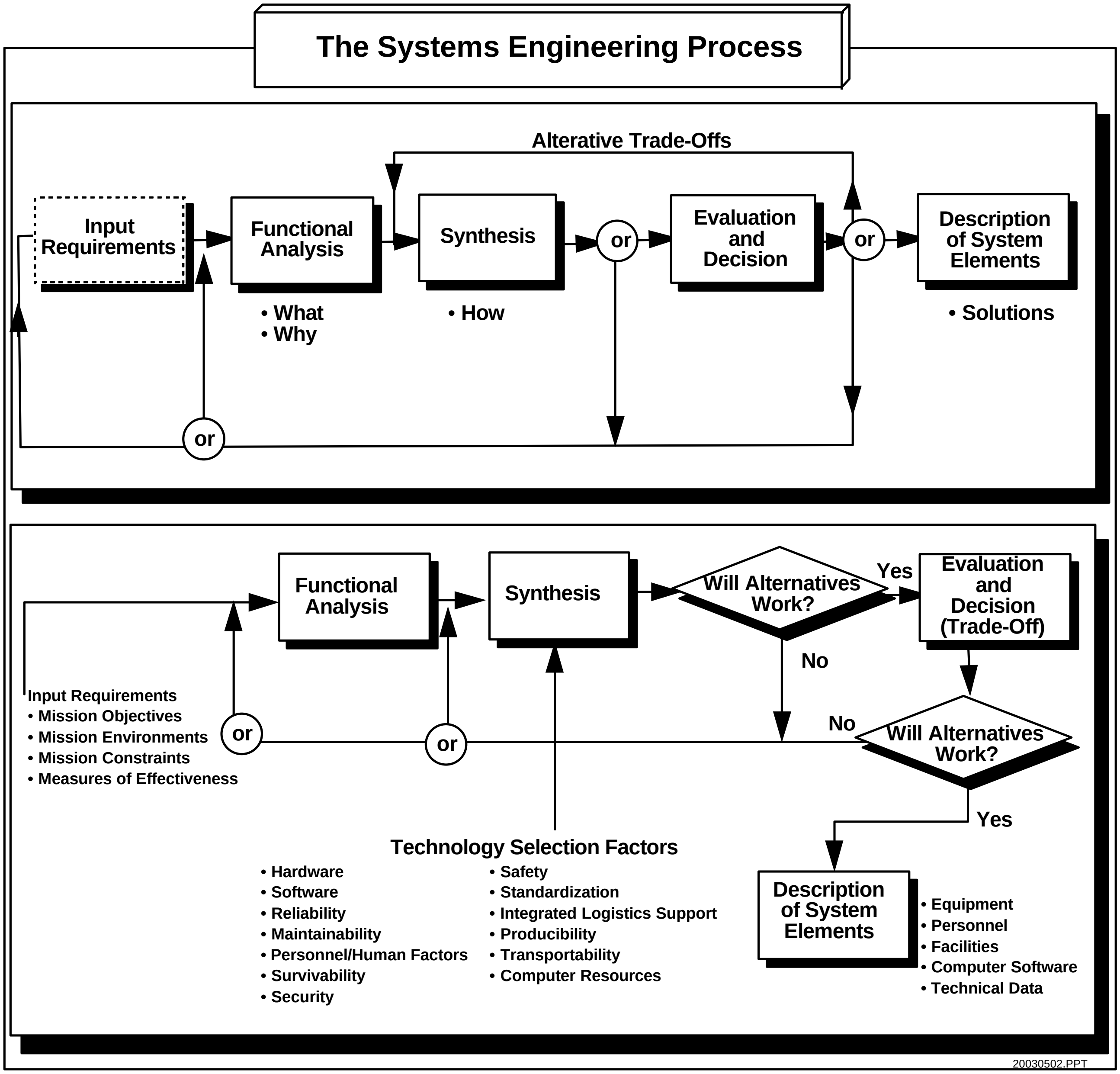

Figure 3-3. The Systems Engineering Process

The acquisition of software commonly follows the LCM process depicted in the DoD 8120 series directives. During concept exploration and definition (Phase 0), the buyer develops requirements, prepares specifications, and develops an acquisition strategy. During source selection, a vendor or developer is chosen to develop the system, based on the proposal made by the vendor or developer. During demonstration and validation (Phase I) and throughout the remainder of the contract period, the vendor's or developer's progress and compliance with contract provisions are monitored.

3.16.1 Planning the Acquisition

Software acquisition planning begins when the requirements start to be prepared (see Sections 3.3, 3.11, and 3.15.1). Because of the lead times involved in competitive procurement, the buyer and seller resources must be put into place well in advance of the contract. The program manager, once in place, is also well advised to immediately begin planning the acquisition and development activities for the remainder of the LCM process. There are two key planning documents in any software acquisition: the PMP and the SDP. The PMP is prepared by the Government and sets the tone for the entire acquisition/development, whereas the SDP, prepared by the contractor, focuses on software methods, tools, and resource issues, and provides the detailed information on how the software will be developed. The key considerations that the PMP and SDP should address include organization and interfaces, activity structure, schedule and milestones, resources, support, subcontractor management, software methodology, reviews, documentation, software environment, testing, product evaluations, and risk management.

The primary planning tool is the WBS (see Section 3.13.1), which should be outlined in the RFP (see Section 3.14.1). Once the WBS has been defined, each of the tasks identified within it can be scheduled, and resources can be estimated.

3.16.2 Life-Cycle Standards

The mechanism used to structure the software acquisition process (including software development) and define the major activities associated with it is the life-cycle model selected for the acquisition. The life-cycle model is a process model and mechanism for communicating to the managerial, technical, and user personnel associated with the program or project what work tasks need to be accomplished, when, and by whom. The most widely used life-cycle process model for software development is the waterfall life-cycle model. While advanced models may be used to structure the work in complex software developments (e.g., the spiral model may be used to incorporate prototyping as a risk reduction option at any stage), the waterfall model can be used to communicate the sequence of events and work that must be accomplished to develop a software product. This model has been institutionalized in a number of standards that provide a basis for management, thus supplying an acquisition infrastructure for the program or project. These standards are among the popular sources of life-cycle process standards contained in TAFIM Volume 7, Appendix A, “Adopted Information Technology Standards (AITS) Table” and in the AITS companion document, the *Information Technology Standards Guidance (ITSG)*.

MIL-STD-498, *Software Development and Documentation*, is the most widely used standard for software development and life-cycle management. It is a management and engineering standard that sets forth requirements for software development and prescribes a uniform software development process. It contains requirements for software development management, software engineering, configuration management, product evaluation, formal qualification testing, transitioning software to the operational environment, and content and format requirements (DIDS) for software data deliverables, the documentation that establishes the baselines to be used to control system design and development. As with all standards selected for a program, tailoring of this standard is recommended (see Sections 3.5 and 3.14.3).

3.16.3 Software Management Environment

The program organization responsible for the management of software development or acquisition should be a highly visible part of the program structure and high enough in the organizational hierarchy to command the resources necessary to do its job effectively. Lines of communication in the program should be structured to expedite vertical as well as horizontal flows. Cross-functional teams also aid in problem resolution involving cross-organizational boundaries. Working groups also aid in problem resolution. Plans to change the organizational structure as the program moves from definition through testing to operations should also be made, so that the right resources are available to perform and support planned activities in each life-cycle phase.

An adequate software environment is also required in both developer and customer organizations. A software environment consists of the set of hardware, software, and firmware used to perform the development effort. Typical elements of the environment include equipment (workstations, file servers, communications networks, etc.), assemblers, compilers, database managers, debuggers, editors, library systems, simulators, CASE tools, and a variety of other tools. Communications are enhanced when both the development organization and the customer have access to the same information stored within the environment.

3.17 INTERFACE MANAGEMENT

Interface definition, management, and control are integral parts of the systems engineering and configuration management processes. Systems engineering is concerned with the identification, documentation, and management of all functional and technical interfaces of a system, its components, support equipment, operating/applications software, and facilities. Interface control is achieved through the CM process as interface requirements are baselined, proposed, and changed. Interface management of an Open System will most likely involve the acquisition of hardware and the development of software applications that will interface with other systems and subsystems. This will require effective interface management to be implemented in the systems engineering and CM processes, to identify and document interfaces, ensure hardware/software standardization, resolve interface problems, and adhere to functional/technical interface requirements. Interface management should be implemented in accordance with the configuration management plan of the program and any and all agreements made between the interfacing parties to ensure interfaces are identified and documented in system design documentation and controlled during system development and operations.

3.17.1 Interface Types

An interface, as defined in MIL-STD-973, is “the functional and physical characteristics required to exist at a common boundary.” In other words, an interface is “identified” when a common boundary exists between two system entities. It is “defined” when characteristics are completely specified (i.e., functional, physical, protocol, performance, data source/destination, frequency/timing levels, data format/content/rate/volume, security characteristics, etc.). The following are the types of interfaces that are typically controlled in an OSE:

- **External interface.** An interface that exists between hardware, software, or both, where design and/or in-service support responsibilities for the two sides of the interface are under the control of different DoD and/or DoD Component activities.

- **Internal interface.** An interface that exists between hardware, software, or both, where design and/or in-service support responsibilities for the two sides of the interface are under the control of the same DoD Component activity and may involve different contractors.

- **Single-entity interface**. An interface that exists between hardware, software, or both, where design and/or in-service support responsibilities for the two sides of the interface are under the control of the same DOD Component activity and the same contractor.

3.17.2 Interface Requirements

Interface requirements must be included in system and development specifications. The development specifications may further allocate interface requirements to lower-level Components, where these requirements will be functionally and physically met. System interface agreements (SIAs) (or other documents deemed as interface control documentation [ICD] for a program) are typically developed for each system application in order to depict the functional and physical interfaces of related or co-functioning items. The SIA/ICD provides the means to measure, evaluate, and formally control the record layout/structure of system data transmissions and record interface agreements between functional areas. The SIA/ICD also serves as the primary document for system interface control and becomes part of the program's technical baseline. A separate SIA/ICD should be developed for each automated interface and updated as a living document throughout the applications life-cycle.

3.17.3 Interface Control

The program's systems engineering management organization and the designer/developer/integrator of the system are jointly responsible for the identification and control of the system's external, internal, and single-entity interfaces. This joint responsibility may be managed through the SIAs/ICDs described above, and by the establishment of an Interface Control Working Group (ICWG), a recommended mechanism for ensuring interface control. The ICWG typically consists of Government and contractor representatives, and representatives from the respective functional areas interfacing with the system at hand. The role of the ICWG is to resolve interface management issues and assess and determine data transfer requirements, including the data needed to meet those requirements. The ICWG normally performs interface management and control tasks from Milestone I to Milestone III.

3.17.3.1 Interface Change Control

Changes to a system application and/or interfacing system during development, testing, or implementation that affect the communications link between organizations or other interface-related issues are typically handled through the program's configuration management organization. Changes and related issues include procedural modifications, hardware or software changes, data element standardization changes, changes to editing criteria, input or output format changes, and frequency of use deviations. The organization assigned as the technical lead for a configuration against which a proposed change is issued ensures interface impact and potential related change analysis through the ICWG. The ICWG determines that interface change requirements have been properly assessed and documented in related change documentation before the technical lead organization approves the basic change. The requirements for the identification, documentation, and coordination of related engineering changes are further defined in MIL-STD-973 (Section 5.4.2.3.6 and Section 6).

3.18 TEST AND EVALUATION

Test and Evaluation (T&E) is an iterative process of measurement, analysis or feedback, corrective action, and retest. It is used throughout the LCM process to reduce technical and program risk and to provide early and continuing estimates of the system's operational effectiveness and suitability. Issues and criteria are developed from operational requirements and performance thresholds and objectives found in early program documents, such as the MNS, program baseline, and requirements documents. Test methods and measurement include data collection (including field test, test beds, and simulations) designed to evaluate the conformance of system components to standards of performance. From a systems engineering perspective, test planning, testing, and analysis of test results are integral parts of the basic systems engineering process. T&E encompasses relationships with all system elements, such as equipment, software, facilities, personnel, and procedural data.

The successful accomplishment of T&E objectives is a key requirement for milestone decisions to commit additional resources to a program or to advance the program from one life-cycle phase to the next. In this respect, test planning needs to be initiated early in the LCM process so that appropriate test activities can be fully integrated into the overall development process.

T&E programs for C4I and information systems fall under the responsibility of the DoD Director, Test and Evaluation (D, T&E) and DoD Director, Operational Test and Evaluation (D, OT&E). Both organizations coordinate and develop and maintain DoD-level T&E policies, procedures, and other guidance by which C4I and information system test programs are assessed and validated through the milestone review process. T&E policy and procedures, described in DoDD 8120.1 and 8120.2 direct the establishment of a T&E program in accordance with the DoD 5000 series directives, in particular DoDI 5000.2, which further identifies the responsibilities for test program oversight, the requirements and guidelines for Developmental Test & Evaluation (DT&E) and OT&E, the major categories of T&E to be implemented. Additionally, DoD 8120.2-M, Part 7, provides procedures and formats for preparing the TEMP, which documents the overall structure and objectives of the T&E

program. A brief overview of the TEMP and the functions of DT&E and OT&E follow in the subparagraphs below.

3.18.1 Test and Evaluation Master Plan

The Test and Evaluation Master Plan (TEMP) is a broad, top-level plan detailing all major T&E events and is a primary document used in the LCM review and decision-making process. The TEMP covers the program life-cycle from initiation through post deployment, including major modifications or upgrades, and defines how the system components will accomplish the planned testing and evaluation for each life-cycle phase in order to support major program decisions. It identifies special T&E resources and requirements to facilitate long-range planning, including the cost of contracted telecommunications, training, Automated Data Processing (ADP), and consulting services; documents major agreements between the material developer and the independent operational T&E agent, and includes the rationale and schedule for planned tests. It also relates the T&E effort clearly to technical characteristics, technical risk, operational issues and concepts, system performance, reliability, availability, maintainability, logistics requirements, and major decision points. A program's first, preliminary TEMP is submitted in support of the Milestone I decision. TEMP updates are then required before each subsequent decision milestone. Additional updates are required when the program baseline is breached or when the program has changed significantly.

The DoD guidelines for TEMP coordination and approval are contained in DoDD 8120.1, DoDI 8120.2, and DoD 5000.2. TEMP preparation is in accordance with the required and specified format of DoD 8120.2-M, Part 7. For multi-service or joint programs, a single, integrated TEMP is required, with requirements unique to a DoD Component annexed to the basic TEMP. For Multi-system programs, a Capstone TEMP integrating the T&E program for the entire system is prepared.

3.18.2 Developmental Test and Evaluation

The Developmental Test and Evaluation (DT&E) is conducted throughout the LCM process to ensure the acquisition and fielding of an effective and supportable system. DT&E is normally planned, conducted, and monitored by the developing agency (joint responsibility of the program manager and contractor) to:

- Assist the design and development process
- Verify performance objectives and specifications
- Demonstrate that design risks have been minimized
- Estimate the system's utility
- Provide assurance that the system/equipment/component is ready for testing in the operational environment.

DT&E includes the T&E of components and subsystems at all WBS levels, including hardware/software integration, related software testing, and production acceptance testing. It emphasizes the use of controlled conditions and well-trained operators and maintainers, and may involve the use of simulations, models, test beds, full-scale engineering development models, and prototypes of system components or the system itself. DT&E can include conformance testing, which includes testing products to the requirements of an Open System interface standard developed through, and approved by, independent standards bodies (i.e., National Institute of Standards and Technology[NIST], ISO, IEEE, ANSI); interoperability testing, which involves the testing of two or more interface-connected products for their ability to work together; and performance testing, which includes the verification of interface performance criteria. While its goal is to verify the attainment of technical performance specifications and objectives, feedback from DT&E results provides meaningful input to risk assessment decision-making.

DT&E is conducted during the concept exploration and definition phase (Phase 0), to assist in selecting preferred alternative system concepts, technologies, and designs. During the demonstration and validation phase (Phase I), DT&E is conducted to identify and validate the preferred technical approach, including the identification of technical risks and feasible solutions. During development (Phase II), DT&E should demonstrate that engineering is reasonably complete, that all significant design problems have been identified with solutions in hand, and that the design meets the required specifications in all areas, such as performance, reliability, and maintainability, within the range of parameters specified for operational deployment. After the Milestone III decision (production and deployment, Phase III), DT&E is an integral part of the development, validation, and introduction of system changes undertaken to improve the system, to react to new requirements, or to reduce life-cycle costs.

3.18.3 Operational Test and Evaluation

For major systems, Operational Test and Evaluation (OT&E) is typically conducted by a major OT&E field agency located within the DoD Component. This operational test agency (OTA) must be separate and independent from both the developing/procuring agency and the using agency. The OTA is responsible for managing operational testing, reporting test results, and providing its independent evaluation of the system being tested to the Military Service Chief or Defense Agency Director for Operational Test and Evaluation, who will approve the organizational structure of the OTA. The principal objectives of OT&E are to:

- Estimate the operational effectiveness and operational suitability of the system
- Identify needed modifications or improvements
- Provide information on tactics, doctrine, organization, and personnel requirements
- Provide data to uphold or verify the adequacy of various manuals, handbooks, supporting plans, and documentation.

OT&E is planned and conducted in an environment as realistic as possible, and can be combined with DT&E when significant, clearly identified cost and schedule benefits will result. Typical operation and support personnel should be used to obtain a valid estimate of the user's capability to operate and maintain the system when deployed; however, the contractor is precluded by public law from participating in realistic OT&E. Operational testing is conducted during the concept exploration and definition phase (Phase 0) to estimate the operational impact of candidate technical approaches and to assist in selecting alternative preferred concepts; during the demonstration and validation phase (Phase I), to examine the operational aspects of the selected alternatives, estimate the potential operational effectiveness and suitability of the candidate system, and identify operational issues for early assessment and future operational testing; during development (Phase II), to demonstrate the system's operational effectiveness and suitability; and after the Milestone III decision (production and deployment, Phase III), to test the fixes to be incorporated into the production or deployment system and to validate the achievement of program objectives.

Although OT&E is planned and conducted by an independent testing activity, the program manager must closely coordinate all aspects of test and evaluation with the OTA, to ensure that DT&E objectives coincide with OT&E objectives.

3.19 LOGISTICS MANAGEMENT

Integrated Logistics Support (ILS) is defined as a composite of the elements necessary to assure the effective and economical support of a system or equipment at all levels of maintenance for its programmed life-cycle. It integrates logistics support elements into complementary time-phased and mission-oriented actions to plan, develop, acquire, and operate equipment. It is implemented as a disciplined, unified, and iterative approach and process to the management and technical activities necessary to integrate support considerations into system and equipment design; develop support requirements; acquire the required support; and provide the required support during operations, at minimal cost. As with other conventional acquisition approaches, ILS is critical to C4I and information system acquisitions, in order to ensure that system design is influenced by support requirements and that support is available for operational sustainment.

The program manager establishes an ILS program in accordance with the requirements of DoDD 5000.2, Part 7, Section A, and may include such ILS areas as logistics support analysis (LSA) and Planning (in accordance with MIL-STD-1388-1B); reliability, availability, and maintainability; supply support, test, and support Equipment; transportation and handling; personnel and training; facilities; technical data and publications; post-production support; and the development of ILS documentation such as the ILSP, Logistics Support Analysis Records (LSAR) (in accordance with MIL-STD-1388-2B), and the Deployment Plan. The overall foundation and objectives of the ILS program are contained in the ILSP, which is developed in accordance with DoD 8120.2-M, Part 13.

3.19.1 Integrated Logistics Support Plan

The Integrated Logistics Support Plan (ILSP) is a management tool that delineates anticipated future logistical planning actions by the program office and external supporting activities. Its function is to identify what logistics support tasks will be accomplished, how and when they will be accomplished, and who will be responsible for their accomplishment. The ILSP is considered the foundation document for coordinating logistics planning efforts to ensure that each of the ILS elements is addressed and integrated with the other program elements throughout the life-cycle. It contains the details that form the basis for specific actions by supporting activities and for developing logistics requirements to be included in contractual documents. The ILSP provides for coordinated actions on the part of logistic element managers and the contractor, and it documents the manner in which each logistic support element is to be obtained, integrated, and sustained.

The program manager is responsible for initiating the ILSP at the outset of the program, in the concept exploration and evaluation phase (Phase 0). The content and format may vary according to Service and should be subject to tailoring, based on program nature and needs. The planning should be focused to the subsystem level and should include the coordination and input of all required and participating staff agencies. When approved, the ILSP becomes the implementation plan for all participating activities and is treated as an integral part of the Program Management Plan. The ILSP should be updated when new program direction is received, when changes involving personnel, training, facilities, and other ILS elements occur, and when there are major system configuration changes.

3.20 METRICS

The increasing complexity of DoD systems, the need for evolutionary or incremental developments, and the migration of legacy systems have traditionally made program management and development a difficult task in itself. Overlaying additional requirements (i.e., imposition of reuse, new development methodologies, languages, processes, and environments) on top of these life-cycle elements further complicates a manager's role and responsibilities. Furthermore, new demands created by complex mission support activities, cross-functional interfaces, Open System requirements, and standards are added burdens to a manager's sphere of operation and influence. Thus, the issue of quantification through metrics application (i.e., understanding what to measure and collect and when to collect it), becomes a significant task in light of the extensive and multiphased life-cycles that drive a particular system development.

A metric is a quantitative value or set of values derived from measurement data that provides an indication of progress, product quality, or resource utilization. Measurement data is quantitative data that directly characterizes some aspect of a project. Metrics application is an important means of monitoring and evaluating the progress of any work effort. Proper use of metrics data can help to manage development, mitigate risks, control costs, and avoid problems.

The various types of metrics that may be employed in a program are briefly discussed in the sections that follow. A more extensive discussion of metrics and their effective use can be found in the following publications: *Practical Software Measurement, DoD Software Performance Engineering (SPE) Project, Software and Performance Metrics Assessment*.

3.20.1 Reuse Metrics

The many variations and deviations of the particular acquisition and development paradigm can easily alter the sequence of events (e.g., design reviews), and the type of information needed for an event or milestone activity (i.e., Milestone I, II, III, or IV). Development under a reuse paradigm requires an earlier review of specific software and design elements, by virtue of their existence, to establish feasibility of the identified reusable software component. It is in the best interests of the program manager and DoD to have a set of measures and metrics on a particular reusable element attesting to its integrity, reliability, and liabilities. The same concept of prior knowledge, quantification, or assessment applies to a contractor selected for the system development in terms of the contractor's ability to develop software of a certain complexity or size. The same argument can be made for the development processes to be encountered, their stability, and their maturity.

3.20.2 Requirements Metrics

Requirements and their related issues and maturity exist in the systems, software, and hardware phases of the life-cycle. Their traceability is of concern to systems, software, and hardware engineers. The collection of requirements metrics should be similar and defined in a consistent manner. Thus, program managers should be aware of the potential for instrumentation across more extensive life-cycle activities and domains, and should focus on common denominators across these disciplines. Systems requirements decompose into lower-level ones, giving rise to allocated and derived requirements. As requirements mature and stabilize, their numbers increase by orders of magnitude and are dispersed across a system's documentation. Requirements expansion and categorization has been recognized in standards for many years. How to group and associate lower-level requirements into effective testing sets that can subsequently be combined into a minimum set of larger system test sets has always been a difficult issue. These same issues are found across domains (e.g., software, systems, hardware). Requirements maturity, stability, traceability, and testability characteristics have also been difficult to capture in supporting design automation and CASE tools. Focusing on requirements common denominators and their metrics across these domains would be of significant consequence to program managers. Changes in requirements are indicative of changes in scope, resulting in a corresponding cost and schedule impact. An awareness of these common denominators enables the program manager to collect metrics earlier in the life-cycle in a more consistent manner. The ability to collect metrics earlier thus provides for better risk mitigation, effective problem resolution, and cost avoidance. Since the identification of common software and systems engineering metrics is now possible, a more uniform collection, traceability, and analysis of these metrics and a definition of viable metrics programs can be obtained.

3.20.3 Migration Metrics

Migration metrics are becoming increasingly important, since the number of legacy systems being transitioned or updated by DoD is increasing. The migration of systems is expected to continue, since DoD resources to build new systems are scarce. Migration of legacy systems becomes even more important in the face of inter-Service operational and cross-functional demands and the need for greater interoperability and use of open standards.

3.20.4 Software Metrics

Software performance metrics are worthwhile and should begin to be incorporated into a software projects metrics program from cradle to grave. These metrics can have a significant impact on the design of software systems when software performance models are applied in the concept and requirements phases. Projecting performance requirements may warrant complete design changes before costly implementation.

Six common metrics have been identified for SPE:

- Response Time
- Throughput
- Workload Specs
- Resource Usage
- Transaction Frequency
- Capacity.

These metrics are the most useful and should be used throughout the system life-cycle process. Estimates should be provided in the concept exploration and evaluation through development phases, and actual measurements should be taken during implementation, test, integration, and operations and maintenance.

3.21 REUSE

Reuse simply means “to put or bring into action or service again or to employ for or apply to a given purpose again.” When properly planned for and exploited, reuse can provide effective leverage to a manager when applied to the following areas:

- Architectures
- Specifications
- Requirements

- System design
- Software.

The concept of reuse has existed for many years. The COSMIC Repository[5] started by NASA over a decade ago to make computer programs available to the public, formalized the reuse repository concept. The NASA monthly publication entitled “NASA Tech Briefs” continues to identify and regularly update the reusable components available and new releases (including new technologies) included the NASA COSMIC Repository.

Over the years, reuse has been recognized as providing both leverage and an additional burden and cost factor to program managers; however, true cost savings can be achieved when reuse initiatives are invoked early in the system life-cycle, when designs and architectures are being developed. While the potential savings to be accrued by developing under a reuse paradigm can be significant, it should be noted that supporting standards are virtually nonexistent, and accompanying program management guidebooks on reuse are in their infancy.

3.21.1 DoD Reuse Repositories

In recognition of the dual nature of reuse and in an effort to contain costs, DoD has established and is continuing to establish reuse repositories. The initial efforts focused on identifying software (i.e., code) for inclusion in the repositories. Subsequently, life-cycle data collected over the years and on various projects revealed that greater leverage from reuse could be obtained if reusable components, other than code, could be included in such repositories (e.g., architectural components, design, specifications, requirements). Reusable components fall into three basic categories: 1) use of the reusable component as-is, without any modifications; 2) use of a parameterized reusable component (i.e., can be used within the range of parameterized inputs or outputs); and 3) modification or redesign of a reusable component. In all cases, basic concerns about issues of liability and warranties have surfaced and must be answered before a reusable component is employed in a program. Statistics on the extent of prior usage and previous histories of the reusable component may provide a measure of added confidence when using the particular item. Identification of reuse metrics also provides insight to subsequent use of reusable components and corporate histories (see Section 3.20).

Additionally, the introduction of formal software engineering methods and techniques into the systems engineering arena has provided program managers with additional analytical and reusable capabilities. The introduction of formal languages (i.e., supported by a syntax) and methodologies into systems engineering has provided the capability to develop other system reusable components in a quantifiable and classifiable manner for repository inclusion and subsequent exploitation. Extending classification schema from repository to other engineering areas (e.g., hardware, firmware) can provide more extensive repositories. Significant productivity and cost savings across the life-cycle may also result from the timely construction

---

[5] The COSMIC Repository resides at the University of Georgia, 382 East Broad Street, Athens, Georgia 30602, Phone (706) 542-3265.

of prototypes (containing design, hardware, and software) that mirror the target system and its requirements very closely.

A current listing of key reuse repositories within the DoD can be found in the *Information Technology Standards Guidance (ITSG)* document, which supports TAFIM Volume 7.

3.22 QUALITY ASSURANCE

Development and execution of a Quality Assurance (QA) program is the responsibility of the program manager. QA program objectives are to: 1) ensure mission and operational effectiveness, user performance, and ownership satisfaction with DoD products; 2) ensure all services and products meet mission and operational needs; 3) ensure essential functional performance and related physical requirements are consistent with needs; 4) ensure contractual requirements are tailored in compliance with DoD direction for specifications and standards; and 5) ensure the other four objectives are cost-effective.

Quality assurance is also the responsibility of all program participants and a requirement of the FAR, which requires the contractor to ensure total contract conformance (product design, manufacture, verification, and delivery). In addition to the contractor, two other independent organizations are involved in QA functions: the Government contracting administration and the program management office. Contract administration or the contracting office is responsible for performing procurement QA, which encompasses accepting the contractor's verification system or quality program, ensuring compliance with all contract requirements, evaluating evidence of product conformance, and performing verification of product conformance before final acceptance. The program office is responsible for ensuring user needs have been translated into enforceable design-to or build-to requirements; participation in design and production readiness reviews; and evaluation of contractor performance in meeting functional and physical uniformity requirements.

Contract provisions for quality include contractor inspection provisions, as on some COTS items and the Standard Inspection Clause, which gives the contractor responsibility for all inspections and tests necessary to ensure contract conformance. The Government may reserve the right to perform any or all inspections and tests before acceptance or to request contractor records for verification. Other higher-level requirements include MIL-I-45208A, *Inspection System Requirement*, used in conjunction with the Standard Inspection Clause, which requires the contractor to establish and maintain a formal, documented inspection system, including vendor control. MIL-Q-9858A, *Quality Program Requirements*, also used in conjunction with the Standard Inspection Clause, obligates the contractor to have a formal quality program. The ISO 9000 series (including ISO Standards 9001 through 9004) describes and clarifies quality concepts and provides guidelines for the selection and use of the other related standards, which identify requirements for a quality management system.

ISO 9001 covers design, development, production, installation, and servicing. The ISO 9002 examines the manufacturer's capabilities in production and installation only, and ISO 9003 focuses on final inspection and testing procedures. ISO 9004 examines each of the quality-system elements in ISO 9000 to help manufacturers set up a quality system; however, this standard is for guidance and should not be contractually imposed.

Quality assurance is also the responsibility of all program participants and a requirement of the FAR, which requires the contractor to ensure total contract conformance (product design, manufacture, verification, and delivery). In addition to the contractor, two other independent organizations are involved in QA functions: the Government contracting administration and the program management office. Contract administration or the contracting office is responsible for performing procurement QA, which encompasses accepting the contractor's verification system or quality program, ensuring compliance with all contract requirements, evaluating evidence of product conformance, and performing verification of product conformance before final acceptance. The program office is responsible for ensuring user needs have been translated into enforceable design-to or build-to requirements; participation in design and production readiness reviews; and evaluation of contractor performance in meeting functional and physical uniformity requirements.

Contract provisions for quality include contractor inspection provisions, as on some COTS items and the Standard Inspection Clause, which gives the contractor responsibility for all inspections and tests necessary to ensure contract conformance. The Government may reserve the right to perform any or all inspections and tests before acceptance or to request contractor records for verification. Other higher-level requirements include MIL-I-45208A, *Inspection System Requirement*, used in conjunction with the Standard Inspection Clause, which requires the contractor to establish and maintain a formal, documented inspection system, including vendor control. MIL-Q-9858A, *Quality Program Requirements*, also used in conjunction with the Standard Inspection Clause, obligates the contractor to have a formal quality program. The ISO 9000 series (including ISO Standards 9001 through 9004) describes and clarifies quality concepts and provides guidelines for the selection and use of the other related standards, which identify requirements for a quality management system.

ISO 9001 covers design, development, production, installation, and servicing. The ISO 9002 examines the manufacturer's capabilities in production and installation only, and ISO 9003 focuses on final inspection and testing procedures. ISO 9004 examines each of the quality-system elements in ISO 9000 to help manufacturers set up a quality system; however, this standard is for guidance and should not be contractually imposed.

This page intentionally left blank.

APPENDIX A

ACRONYMS

A&T	Acquisition and Technology
ADP	Automated Data Processing
AFR	Air Force Regulation
AIS	Automated Information System
AITS	Adopted Information Technology Standards
AMSDL	Acquisition Management Systems and Data Requirements List
ANSI	American National Standards Institute
AR	[1] Adjunct Requirement [2] Army Regulation
ASCII	American Standard Code for Information Interchange
ASD	Assistant Secretary of Defense
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computer and Intelligence
CASE	Computer-Assisted Software Engineering
CCB	Configuration Control Board
CDAd	Component Data Administrator
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDS	Concept Design Sheet
CI	Configuration Item
CIM	Corporate Information Management
CISS	Center for Information System Security
CLIN	Contract Line Item Number
CM	Configuration Management
COTS	Commercial-off-the-Shelf
CPR	Cost Performance Report
C/SCSC	Cost/Schedule Control System Criteria
C/SSR	Cost/Schedule Status Report
DAB	Defense Acquisition Board
DAE	Defense Acquisition Executive
DBMS	Database Management System
DDDS	Defense Data Dictionary System
DEPSECDEF	Deputy Secretary of Defense
DFARS	Defense Federal Acquisition Regulations
DGSA	DoD Goal Security Architecture
DID	Data Item Description
DII	Defense Information Infrastructure

DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DISSP	Defense Information Systems Security Program
DoD	Department of Defense
DoD DAd	DoD Data Administrator
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSSP	Defense Standardization and Specification Program
DT&E	Developmental Test and Evaluation
ECP	Engineering Change Proposal
EDM	Enterprise Data Model
EEO	Equal Employment Opportunity
EI	Enterprise Integration
FAR	Federal Acquisition Regulation
FDAd	Functional Area Data Administrator
FEA	Functional Economic Analyses
FIPS	Federal Information Processing Standard
FIS	Facility Interface Sheet
FMECA	Failure Modes Effects and Criticality Analysis
FPI	Functional Process Improvement
FQR	Functional Qualification Review
HCI	Human Computer Interface
HDBK	Handbook
I-CASE	Integrated Computer-Assisted Manufacturing
ICD	Interface Control Document
ICWG	Interface Control Working Group
IDEF	ICAM Definition Method for Integrated Computer System Manufacturing
IEEE	Institute of Electrical and Electronic Engineers
ILS	Integrated Logistics Support
ILSP	Integrated Logistics Support Plan
IM	Information Management
IPR	In-Process Review
IRDS	Information Resource Dictionary System
ISO	International Organization for Standardization
IT	Information Technology
ITSG	Information Technology Standards Guidance

LAN	Local Area Network
LCC	Life-Cycle Cost
LCM	Life-Cycle Management
LSA	Logistics Support Analysis
LSAR	Logistics Support Analysis Record
MAISRC	Major Automated Information System Review Council
MDA	Milestone Decision Authority
MIL	Military
MNS	Mission Need Statement
NCSC	National Computer Security Center
NDI	Non-Developmental Item
NGCR	Next Generation Computer Resources
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OSE	Open Systems Environment
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
PC	Personal Computer
PDR	Preliminary Design Review
PEO	Program Executive Officer
PMO	Program Management Office
PMP	Program Management Plan
PMS	Program Master Schedule
POSIX	Portable Operating System Interface
PRR	Production Readiness Review
PSA	Principal Staff Assistant
QA	Quality Assurance
RAS	Requirements Allocation Sheet
RFP	Request for Proposal
RMP	Risk Management Plan
SBA	Standards-Based Architecture
SBD	Schematic Block Diagram
SDM	System Decision Memorandum
SDP	System Decision Paper
SDR	System Design Review
SECDEF	Secretary of Defense

SECNAVINST	Secretary of the Navy Instruction
SEMP	Systems Engineering Management Plan
SIA	System Interface Agreement
SOW	Statement of Work
SPE	Software Performance Engineering
SRR	System Requirements Review
SSA	Source Selection Authority
SSAC	Source Selection Advisory Council
SSEB	Source Selection Evaluation Board
SSP	Source Selection Plan
SSR	Software Specification Review
STD	Standard
T&E	Test and Evaluation
TAFIM	Technical Architecture Framework for Information Management
TDP	Technical Data Package
TEMP	Test and Evaluation Master Plan
TLS	Timeline Sheet
TPM	Technical Performance Measurement
TRM	Technical Reference Model
TRR	Test Readiness Review
TRS	Test Requirements Sheet
TSR	Trade Study Report
USD(A)	Under Secretary of Defense for Acquisition
WAN	Wide Area Network
WBS	Work Breakdown Structure

APPENDIX B

DEFINITIONS

- To Be Provided -

This page is intentionally left blank.

APPENDIX C

REFERENCES

Note: References appearing in this section represent documents used in preparation of the TAFIM, including some sources used at the time of initial document development that may no longer be current or applicable. The reader is advised to check the current applicability of a reference appearing in this list before using it as an information source. The reference section will be completely reviewed and revised for the next release of the TAFIM.

Federal Regulations

Federal Acquisition Regulation (FAR)

OMB Circular A-76, Supplement 1, Cost Comparison Handbook

OMB Circular A-109, Major System Acquisitions

Defense Federal Acquisition Regulation (DFAR)

DoD Directives (DoDD), Instructions (DoDI), and Manuals (in document number order)

DoDD 4105.62 *Selection of Contractual Sources for Major Defense Systems*

DoDD 4120.3 *Defense Standardization and Specification Program*

DoD 4120.3-M *Defense Standardization Program and Policies, Procedures, and Instructions*

DoD 4245.3 *Design to Cost Manual*

DoDD 4245.7 *Transition from Development to Production*

DoD 4245.7-M *Transition from Development to Production*

DoDD 5000.1 *Defense Acquisition*

DoD 5000.19-L *Acquisition Management Systems and Data Requirements List (AMSDL)*

DoDI 5000.2 *Mandatory Procedures for Major Defense Acquisition programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs*

DoDI 5000.38 *Production Readiness Reviews*

DoDD 5000.40 *Reliability and Maintainability*

DoDD 5000.43	*Acquisition Streamlining*
DoDD 5000.49	*Defense Acquisition Board*
DoD 5000.52-M	*Career Development Program for Acquisition Personnel Manual*
DoDD 5137.1	*Assistant Secretary of Defense, Command, Control, Communications, and Intelligence*
DoDD 5200.1-R	*Information Security Program Regulation*
DoDD 5200.28	*Security Requirements for Automated Information Systems (AIS)*
DoDD 5200.28-M	*ADP Security Manual*
DoDD 5200.5	*Communications Security*
DoDI 7000.2	*Performance Measurement for Selected Acquisitions*
DoDI 7000.10	*Contract Cost Performance, Funds Status, and Cost/Schedule Status Reports*
DoDD 8000.1	*Defense Information Management (IM) Program*
DoD 8020.1-M	*Interim Management Guidance on Functional Process Improvement* (with Change 1)
DoDD 8120.1	*Life-Cycle Management (LCM) of Automated Information Systems (AISs)*
DoDI 8120.2	*Automated Information System (AIS) Life-Cycle Management (LCM) Process, Review, and Milestone Approval Procedures*
DoD 8120.2-M	*Automated Information System Life-Cycle Management Manual*, Draft
DoDD 8320.1	*DoD Data Administration*
DoD 8320.1-M	*Data Administration Procedures*
DoD 8320.1-M-1	*Data Element Standardization Procedures*
DoD 8320.1-M-X	*DoD Enterprise Data Model Development, Approval, and Maintenance Procedures*

DoD and Military Standards (in document number order)

DoD 5200.28-STD	*Trusted Computer System Evaluation Criteria*
MIL-STD-470	*Maintainability Program Requirements for Systems and Equipment*
MIL-STD 490A	*Specification Practices*
MIL-STD-498	*Software Development and Documentation*
MIL-STD-785	*Reliability Program for System and Equipment Development and Production*
MIL-STD-881	*Work Breakdown Structures for Defense Material Items*
MIL-STD-882	*System Safety Program Requirements*
MIL-STD-973	*Configuration Management*
MIL-STD-1388-1A	*Logistics Support Analysis*
MIL-STD-1388-2A/2B	*DoD Requirements for a Logistics Support Analysis Record*
MIL-STD-1472D	*Human Engineering Design Criteria for Military Systems, Equipment and Facilities*
MIL-STD-46855	*Human Engineering Requirements for Military Systems, Equipment and Facilities*

Military Regulations and Instructions (in document number order)

AFR 70-15	"Proposal Evaluation and Source Selection"
AFR 800-11	"Life-Cycle Costing"
AR 715-6	"Proposal Evaluation and Source Selection"
SECNAVINST 4200.33*S*	"Selection of Contractual Sources for Major Defense Systems"

DoD/Military Handbooks (in document number order)

DoD-HDBK-248	*Guidance for Application and Tailoring of Requirements for Defense Material Acquisitions*
MIL-HDBK-61	*Configuration Management Guide*
MIL-HDBK-71A	*Human Engineering Guidelines for Management Information Systems*
MIL-HDBK-245	*Preparation of Statement of Work (SOW)*

Military Specifications (in document number order)

MIL-I-45208A	*Inspection System Requirements*
MIL-T-31000	*Technical Data Packages, General Specification for Int. Amendment 1 (OSD)*
MIL-Q-9858A	*Quality Program Requirements*

Industry Standards (in document number order)

ANSI/IEEE 1042-1987	*Guide to Software Configuration Management*
ANSI/IEEE 828-1990	*Software Configuration Management Plans*
IEEE 1220	*Standard for System Engineering, Draft Rev 1.0,* Institute of Electrical and Electronic Engineers, April 25, 1994
EIA/IS-649	National Consensus Standard for Configuration Management
ISO 9000/ANSI/ASQC 90	*Quality Standards*
ISO 9001	*Model for Quality Assurance in Design/Development/Production, Installation and Servicing*
ISO 9002	*Model for Quality Assurance in Production and Installation*
ISO 9003	*Model for Quality Assurance in Final Inspection and Test*
ISO 9004	*Quality Management and Quality System Elements — Guidelines*

Publications (alphabetically, by title)

Acquisition and Technology (A&T) Architecture Development Handbook, DISA, Draft, March 31, 1995

Acquisition and Technology (A&T) CIM/EI Program Management Structure, DISA, Working Draft, June 12, 1995

Application Portability Profile (APP), The U.S. Government’s Open System Environment Profile Version 3.0 (supersedes NIST SP 500-210), NIST Special Publication 500-XXX, Draft, April 12, 1995

Acquisition How To Guide, DISA, August 1993

Architecture Relationships and Definitions, DISA, Draft, June 20, 1995

Defense Information Infrastructure (DII) Strategic Enterprise Architecture, DISA, Coordination Draft, May 31, 1995

DoD Architectures Review, Draft Technical Report, Volume I (abridged), January 30, 1995

DoD Architectures Review, Draft Technical Report, Volume II (unabridged), January 30, 1995

DoD Corporate Information Management for the 21st Century, a DoD Strategic Plan, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I), June 1994

DoD Enterprise Integration (EI) Implementing Strategy, DISA Center for Integration and Interoperability, June 1994

DoD Software Performance Engineering (SPE) Project, DISA Center for Standards, Draft, July 1995

DoD Software Reuse Initiative Strategic Plan, DISA, June 1995

GCCS Common Operating Environment Requirements, DISA, Draft, August 15, 1994

Guide on Open System Environment Procurement, Gary E. Fisher, NIST Special Publication 500-220, October 1994

Information Technology Standards Guidance (ITSG), Draft, May 31, 1995

NASA Tech Briefs, NASA Digest Publication, Monthly

Next Generation Computer Resources (NGCR) Acquisition Guide, Space and Navel Warfare Systems Command, SPAWAR 331, NGCR Document No. AST 001 ver. 0.11, Draft, March 30, 1995

Practical Software Measurement, Joint Logistic Commanders, JPCGCRM, Draft Coordination Version, April 12, 1995

Software and Performance Metrics Assessment, DISA, Center for Standards, Draft, August 1995

Software Reuse Implementation Guide, Dept. of the Navy, Naval Information Systems Management Center, Draft, May 1993

Structured Management Process for Architecture Development, DISA, Draft, March 31, 1995

Technical Standards for Command and Control Information Systems (CCISs) and Information Technology, NATO, ATCCIS Working Paper 25, Edition 4, February 25, 1994

Memoranda and White Papers (in reverse chronological order)

"Architecture Terms and Definitions," George Endicott and Anthony Simon, OASD(C3I)/CISA, White Paper, June 30, 1995

"Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement," OASD(C3I), Memorandum (with attachment), October 13, 1993

"Selection of Migration Systems," OASD(C3I), Memorandum, January 15, 1993

"Enhancing Defense Standardization-Specifications and Standards: Cornerstones of Quality," Report to SECDEF by USD(A), November 1988

"Acquisition Streamlining," DepSecDef Memorandum, June 3, 1985

APPENDIX D

TAFIM POLICY MEMORANDA

D.1 This appendix contains the text of the following pertinent policy documents addressing the use of the TAFIM as direction and guidance in the evolution of the DoD Technical Infrastructure.

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Memorandum (with attachment), “Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement,” 13 October 1993.

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Memorandum, “Selection of Migration Systems,” 12 November 1993.

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Memorandum, “Technical Architecture Framework for Information Management (TAFIM),” 30 March 1995.

MEMORANDUM FROM
THE DEPUTY SECRETARY OF DEFENSE

13 October 1993

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT TO SECRETARIES OF DEFENSE
COMPTROLLER
GENERAL COUNSEL
INSPECTOR GENERAL
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement

My May 7, 1993, memorandum reiterated the full commitment of the Department of Defense (DoD) to the "...improvements, efficiencies, and productivity that are the essence of CIM." The focus of Corporate Information Management (CIM) on functional process improvement, migration systems, and data standardization has my full support. We need to get on with the job. In order to offset our declining resources, we must accelerate the pace at which we define standard baseline process and data requirements, select and deploy migration systems, implement data standardization, and conduct functional process improvement reviews and assessments (business process re-engineering) within and across all functions of the Department. The acceleration of these actions is key to containing the functional costs of performing the DoD mission within our constrained budget.

The attached guidance requires that addressees expedite selection of standard migration systems and standard data as the basis for process improvement reviews and assessments. The attached guidance expands on direction previously issued by the Comptroller on June 25, 1990, and by the Assistant Secretary of Defense Command, Control, Communications, and Intelligence(ASD(C^3I) on February 11, 1991. The ASD(C^3I) will work with you to ensure that overall functional and Component requirements are met and balanced as we integrate and improve systems, data, and processes across the DoD. Our near-term strategy requires:

- Selection of migration systems within six months, with follow-on DoD-wide transition to the selected systems over a period not to exceed three years.

- Complete data standardization within three years by simplifying data standardization procedures, reverse engineering data requirements in approved and proposed migration systems, and adopting standard data previously established by individual functions and Components for DoD-wide use wherever practical.

The above actions should be implemented immediately, and given appropriate priority in your current and future resource planning and allocation.

Ongoing information management initiatives such as functional process improvement projects, functional and technical integration analysis and planning, and software engineering methods modernization should continue on an expedited basis. However, completion of these current initiatives will not be prerequisites to implementation of the migration system and data standards acceleration strategy. Once standard DoD-wide process, system, and data baselines are established, process improvement studies will be more productive and study results can be more rapidly implemented.

It is understood that the implementation of standard migration systems may result in the loss of automated functionality by selected system users, whereas others may gain functionality. Loss of functionality should not be used as a reason to delay migration system selection and deployment unless there is a documented adverse impact on readiness within the deployment period, or an inability to comply with the law.

The ASD(C^3I) is responsible for supplementing existing procedures with generic evaluation criteria within 30 days to be used in selecting migration systems, and ensuring the objectivity of the selection process.

I request that you personally ensure these actions are accomplished on schedule, and that you report to me on your progress by January 31, 1994.

s/William J. Perry

Attachment

DEPARTMENT OF DEFENSE

STRATEGY FOR ACCELERATION OF MIGRATION SYSTEMS AND DATA STANDARDS

OBJECTIVE

Improve the quality and utility of DoD information while reducing the annual cost of DoD operations.

STRATEGY

Migration Systems

- OSD Principal Staff Assistants, together with their Defense Component counterparts, will, by March 31, 1994, select an information system(s) for each of their respective functional areas of responsibility for designation as the standard, DoD-wide migration system.

- Concurrently, OSD Principal Staff Assistants will develop plans to transition all information technology services throughout the DoD to the selected migration systems, over a period not to exceed three years. Draft plans will be circulated to other Principal Staff Assistants and to Defense Components so that cross-functional and other implementation issues can be identified for consideration by functional and Defense Component members of the DoD corporate Functional Integration Board, chaired by the Deputy Assistant Secretary of Defense (Information Management).

- Funding for development, modernization, or enhancement of legacy systems not selected to be migration systems will be stopped except where approved by the DoD Senior Information Management Official as absolutely essential to support DoD missions or comply with the law.

- The plan for implementing and transitioning services to the selected migration systems should simultaneously forecast a schedule, to the extent practical, for incorporating within the migration systems:

  – Improved functionality and cross-functional integration based on accelerated process improvement reviews and assessments.

  – Interoperability, technical integration, DoD standard data, and integrated databases to provide higher quality and lower cost information technology services for all users.

- Where a requirement is demonstrated to develop a follow-on, new start system to replace the standard migration system in order to meet CIM objectives and the information management policies and principles established in DoD Directive 8000.1, OSD Principal Staff Assistants will conduct the necessary process improvement studies to develop functional requirements within the next three years.

Data Standardization

- Each DoD Principal Staff Assistant, together with their Defense Component counterparts, will develop and execute a plan in accordance with DoD Directive 8320.1 to standardize the data elements for which they are the custodian within the next three years.

- The ASD(C^3I) will, by January 31, 1994, develop simplified and streamlined processes for data standardization and data administration within the DoD.

- In the interim, the Department will continue to use the existing standard data elements within each function and Defense Component that have been developed under previous procedures. These interim standard data elements are the data standards until replaced by those prepared under DoD Directive 8320.1.

DEFINITIONS

The definitions below are intended to clarify the terms used in the DoD near-term strategy for acceleration of migration systems and data standards. Formal definitions are published in DoD directives or other publications.

Baseline Processes and Data

A baseline is something that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. Baseline processes and data establish how a function operates today (the "as is" environment), and what current functional requirements must be satisfied by the supporting migration system. Process improvement projects assess the "as is" baseline to determine what improvements should be made (to the "to be" environment). Once these improvements have been implemented, they define a new process and data baseline for the next iteration of improvements.

Data Standard (also called standard data)

A data element that has been through a formal analysis (called "data standardization") to reach agreement on its name, meaning, and characteristics, as well as its relationship to other standard data elements. Much like a common language, data standards enable processes and their supporting information systems to be integrated across functions, as well as within them, and improve the quality as well as the productivity of enterprise performance.

Data Standardization

The process of reviewing and documenting the names, meanings, and characteristics of data elements so that all users of the data have a common, shared understanding of it.

Data standardization is a critical part of the DoD Data Administration Program, managed under DoD Directive 8320.1. Data administration is the function that manages the definition and organization of the Department's data.

Function

Appropriate or assigned duties, responsibilities, and tasks that produce products or provide services. In the DoD, a functional area (e.g., personnel) is comprised of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviewing candidates). The functions of the DoD are the responsibility of designated officials who exercise authority over organizations set up to accomplish their assigned functions. The structure and interrelationships among DoD functions and standard data are documented in the DoD Enterprise Model.

Individual functions within the DoD rely on other functions for products and services. In a large, complex enterprise such as the Department of Defense, functions must work together to support the mission of the enterprise; this significantly increases the importance of cross-functional programs, such as data standardization.

Functional Process Improvement (also called business process re-engineering)

Application of a structured methodology to define a function's objectives and a strategy for achieving those objectives; its "as is" and "to be" process and data environments; its current and future mission needs and end user requirements; and a program of incremental and evolutionary improvements to processes, data, and supporting migration systems that are implemented through functional, technical, and economic analysis and decision-making.

Procedures for conducting process improvement reviews and assessments in the DoD are provided in OASD(C^3I) memoranda on Interim Management Guidance on Functional Process Improvement (August 5, 1992, and January 15, 1993).

Integration

Explicit top management initiatives to ensure that interdependent functions or systems operate effectively and efficiently for the overall benefit of the enterprise (i.e., the DoD). This contrasts with coordination among functions or systems, which ensures non-interference, but does not provide integration.

"Integration" implies seamless, transparent operation based on a shared or commonly-derived architecture (functional or technical) and standard data. "Interoperability" implies only the ability of a function or system to exchange information or services with another, separate function or system using translators or interchange rules/standards.

Migration System

An existing automated information system (AIS), or a planned and approved AIS, that has been officially designated as the single AIS to support standard processes for a function. Other AISs, called "legacy systems," that duplicate the support services provided by the migration system are terminated, so that all future AIS development and modernization can be applied to the migration system. A migration system is designated (or selected) by the OSD Principal Staff Assistant(s) and their Defense Component counterparts whose function(s) the system supports, with the coordination of the DoD Senior Information Management Official.

Upon selection and deployment, the migration system becomes the single AIS baseline for:

- Incremental and evolutionary changes that are required to implement functional process improvements, or to execute additional responsibilities assigned to the function that the system supports.

- Technical enhancements that implement standard data and integrated databases, and that migrate the system toward an open systems environment and a standards-based architecture defined by the DoD Technical Architecture Framework for Information Management.

Requirements for selection of migration systems are identified in Chapters 6 and 7 of OASD(C^3I) memoranda on Interim Management Guidance for Functional Process Improvement (August 5, 1992, and January 15, 1993); these procedures should be tailored as appropriate to facilitate expeditious selection. Subsequent development and modernization of migration systems is accomplished in accordance with DoD Directive 8120.1 and DoD Instruction 8120.2.

MEMORANDUM FROM
THE ASSISTANT SECRETARY OF DEFENSE

November 12, 1993

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
COMPTROLLER
GENERAL COUNSEL
INSPECTOR GENERAL
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Selection of Migration Systems

This memorandum provides the generic evaluation criteria to be used in selection of migration systems as required by the Deputy Secretary of Defense (DEPSECDEF) memorandum of 13 October 1993, "Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement." The Department of Defense (DoD) must improve the quality and effectiveness of information support for our fighting forces, reduce the cost of duplicative processes, eliminate nonessential legacy systems in all functional areas, and minimize the cost and difficulty of information systems technical integration. Information systems are comprised of applications, data and infrastructure. Expedited selection of migration systems has been established by the Deputy Secretary of Defense as a matter of urgency throughout the DoD. Selection shall be based on these four factors:

- Functional: To be selected as a migration system, the information system will have to be based on defined work processes and will have to be based on the degree to which the system meets the information needs of users within and across functional areas. A decision should be generally supported by the functional user community within the DoD Components, including the Chairman of the Joint Chiefs of Staff (CJCS) representing the unified combatant commands.

- Technical: The system can evolve (migrate) to be supported by the integrated, standards-based architecture prescribed for the future Defense Information Infrastructure (DII).

- Programmatic: A functional economic analysis that documents a reasonable range of alternatives that meet both functional and technical objectives is required. The alternatives must be within programmatic constraints (resources, schedules, and acquisition strategy), and justify adopting the migration system to the Department. Given the compressed time frames, the PSAs may elect to base their migration decision on an abbreviated functional economic analysis. Acquisition strategy planning factors will be considered in accordance with Acting ASD(C^3I) memorandum of February 4, 1993, "Acquisition Strategy Planning for CIM Migration Systems."

- Data: The ability to transition to data standards is a fundamental requirement for an information system in order for it to be selected as a migration system. Applications should lend themselves to data sharing within their design. Migration plans must include transition to DoD standard data and shared data concepts.

Migration systems selection procedures and factors are discussed in our Interim Management Guidance on Functional Process Improvement (August 5, 1992, and January 15, 1993). Except where exempted under DoD Directive 8120.1, Section B, the selection procedures apply to all AISs in the Department. This includes all C^3I systems except those specifically and individually exempted by me in accordance with my DoD Senior Information Management (IM) authority under DoD Directives 5137.1 and 8000.1. All information technology services shall be transition to the selected migration systems over a period not to exceed three years, and the legacy systems providing these services shall be terminated. Any funding for development, modernization, or enhancement of these legacy systems requires the approval of the DoD Senior IM Official, in accordance with the DEPSECDEF's memorandum of October 13, 1993. Life-cycle management reviews of migration systems shall also address these candidate legacy systems and data until their termination.

Migration system selection shall be made by the Office of the Secretary of Defense (OSD) Principal Staff Assistant(s) (PSAs), or CJCS, having functional responsibility for the missions and functions supported by the system, with the participation of affected DoD Components. The choice of functional criteria guidance in the selection of migration systems is the responsibility of the PSAs/ CJCS. As the DoD Senior IM Official, I shall approve the proposed selection, based on my review of the selecting official's evaluation of technical, programmatic, and data factors. Because technical factors are critical to successful implementation of the DII, I shall have additional studies conducted where appropriate, and I shall withhold my approval where significant issues remain unresolved. Disagreements shall be resolved in accordance with DoD Directive 8000.1, Section E.1.d.

Attached to this memorandum are key technical considerations that must be addressed in the selection process. Assistance in your selection of migration systems and in preparation of the appropriate documentation is available through the Defense Information Systems Agency Center for Integration and Interoperability. If you would like this assistance, please contact Dr. Michael Mestrovich at (703) 756-4740.

s/Emmett Paige, Jr.

Attachment

KEY TECHNICAL FACTORS TO BE CONSIDERED IN THE SELECTION OF MIGRATION SYSTEMS

Technical Factors

Extent to which the candidate legacy automated information system (including Command, Control, Communications and Intelligence (C^3I) systems) currently conforms to, or can evolve (migrate) to conformance with, the open systems environment and standards-based architecture defined by the DoD Technical Architecture Framework for Information Management (TAFIM)[1].

Difficulty, cost, and time line for migrating the system (including its applications, data, and supporting infrastructure) as expeditiously as possible from its current technical environment to conformance with:

- The TAFIM
- DoD standard data, based on the DoD Data Model. The DoD Data Model is a principal component of the DoD Enterprise Model
- Shared use of applications, databases, and the computing and communications infrastructure with other designated migration systems
- Cost effective, timely, secure, and highly reliable support to all functional users from consolidated data processing facilities

Timeliness, completeness, and availability of life-cycle management and supporting documentation, particularly including data and application software documentation

Difficulty, cost, and time line for application of:

- DoD information technology utility services
- Commercial-off-the-shelf (COTS) software, and portable, re-usable software modules
- Ada and computer-aided software engineering (CASE) tools and methods

Current and future interface, interoperability, and integration requirements with other systems and databases within and across all DoD functional activities and functional areas.

Application of Technical Factors

---

[1] Office of the Assistant Secretary of Defense (C^3I) Memorandum, “Interim Management Guidance on the Technical Architecture Framework for Information Management (TAFIM),” January 15, 1993.

Application of these technical factors results in giving preference to systems that:

- Have been developed using Ada and other “state of the industry” software engineering best practices, are well documented, and are under good configuration control.
- Use current COTS information technology software and hardware, such as data dictionaries and data base management systems, optical disk technology, etc.
- On the whole, are more compliant rather than less compliant with the technical factors listed above, and apply those factors consistently across all systems supporting the functional area.

Assessment and Plans

The selection of a candidate migration AIS must be founded on its functional and technical adequacy. Migration assessment includes a technical analysis of migration candidate systems to ensure legacy applications will meet the information requirements of the functional user and that has the ability to accommodate subsequent functional and technical improvement activities.

A migration plan consisting of functional, technical and data concerns, with programmatic considerations is the start of the process for selecting migration systems. The DoD “Tree” diagrams, a quarterly publication from DISA/Center for Integration and Interoperability (CFII), displays each functional area’s decisions for integrating. These “Tree” diagrams will be completed by all functional areas with target dates to depict the Enterprise Integration. The diagrams present an important migration picture but stop short of the migration planning that is necessary for implementation. The DISA/CFII is available to help each functional area develop migration plans and assess technical cross-functional integration for the Enterprise.

To validate the technical sufficiency of a candidate migration system, the applications should be evaluated in terms of relevant functional, technical, data handling, and programmatic criteria.

MEMORANDUM FROM
THE ASSISTANT SECRETARY OF DEFENSE

March 30, 1995

MEMORANDUM FOR UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARY OF THE ARMY (RD&A)
ASSISTANT SECRETARY OF THE NAVY (RD&A)
ASSISTANT SECRETARY OF THE AIR FORCE
(ACQUISITION) (SAF/AQ)
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, JOINT STAFF

SUBJECT: Technical Architecture Framework for Information Management (TAFIM), Version 2.0

My memorandum dated June 23, 1994 established the TAFIM as the single framework to promote the integration of Department of Defense (DoD) information systems, expanding the opportunities for interoperability and enhancing our capability to manage information resources across the Department. The latest version of the TAFIM, Version 2.0, is complete and fully coordinated. Version 2.0 consists of seven volumes as shown in the attachment. The TAFIM will continue to guide and enhance the evolution of the Department's information systems technical architectures.

I want to reiterate two important points that I made in my June 1994 memorandum. First, the Department remains committed to a long range goal of an open systems environment where interoperability and cross functional integration of our systems and portability/reuseability of our software are key benefits. Second, the further selection and evaluation of migration systems should take into account this long range goal by striving for conformance to the TAFIM to the extent possible.

Effectively immediately, new DoD information systems development and modernization programs will conform to the TAFIM. Evolutionary changes to migration systems will be governed by conformance to the TAFIM.

The TAFIM is maintained by the Defense Information Systems Agency (DISA) and is available electronically via the DISA On-Line Standards Library. Hardcopy is available through the Defense Technical Information Center. The TAFIM is an evolving set of documents and comments for improving may be provided to DISA at any time. The DISA action officer is Mr. Bobby Zoll, (703) 735-3552. The OSD action officer is Mr. Terry Hagle, (703) 604-1486.

s/Emmett Paige, Jr.

Attachment

APPENDIX E

SYSTEMS ENGINEERING ELEMENTS/ACTIVITIES AND PRODUCTS

E.1 The following table identifies and describes the major elements/activities and products of the Systems Engineering discipline discussed in Volume 5, Section 3.15. In addition to the traditional systems engineering elements, the table includes summaries of those engineering disciplines that are considered engineering specialties influencing and supporting the design, development, and operational support of the system. For C4I and information systems programs, engineering specialties may include logistics engineering, reliability and maintainability engineering, human factors engineering, safety engineering, as well as others not included in the table, which are integrated into the system design and development processes through the systems engineering process. The table also includes the governing standards and other resources for each activity that provide more detailed information and guidance on system engineering requirements and implementation.

Table E-I. Systems Engineering Elements/Activities and Products

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
Requirements Analysis **See Section 3.3 for the description of Requirements Analysis.**	- System Level Functional Requirements - Performance Requirements - External Interfaces	DODI 5000.2, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs)and Major Automated Information System (MAIS) Acquisition Programs*.
Functional Analysis/Allocation Forms the foundation for systems engineering and is the method for analyzing performance requirements and devising them into discrete tasks or activities. Involves identification and decomposition of the primary top-level system functions into subfunctions at ever-increasing levels of detail; supports mission analysis in defining functional areas and architectures, sequences, and interfaces; and is used to develop requirements for equipment, software, personnel, and operational procedures to complete implementation and deployment of the system. Should result in a baseline of functions and functional performance requirements, which must be met to adequately accomplish the operation, support, test, and production requirements of the system.	- System Level (Type A) specification - Functional Flow Block Diagrams - N^2 diagram - Timeline Analysis/ Timeline Sheet (TLS) - Mathematical models and computer simulations, if necessary - Requirements Allocation Sheet (RAS), Test Requirements Sheet (TRS), Facility Interface Sheet (FIS), etc. - Logistics Support Analysis Record (LSAR)	MIL-STD 490A, *Specification Practices*; MIL-STD-1388-1A, *Logistics Support Analysis*; MIL-STD-1388-2A/2B, *DoD Requirements for Logistics Support Analysis Record*. DODI 5000.2, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*.

Systems Engineering Elements/Activities	**Outputs/Products**	**Governing Standards/Guidance**
Design Synthesis and Verification (Conceptual Design) Synthesis is “the performance, configuration, and arrangement of a chosen system and its elements and the technique for their test, support, and operation, all of which to be portrayed in a suitable form such as a set of schematic block diagrams, physical and mathematical models, computer simulations, layouts, detailed drawings, and similar engineering graphics. These portrayals typically illustrate intra- and inter-system and item interfaces, permit traceability between elements at various levels of system detail, and provide the means for complete and comprehensive change control. They are also the basic source of data for developing, updating, and completing the system and configuration items, and for critical item specifications; interface control documentation; consolidated facility requirements; procedural handbooks, and similar forms of instructional data; task loading; operational computer programs; specification trees; and dependent elements of work breakdown structures”. Additionally, through synthesis, architectures are transformed from functional to physical; alternative systems concepts, configuration items, and system elements are defined; physical interfaces (internal and external) are defined and refined; and preferred product and process solutions are selected. The results of various technical and design studies as well as requirements delineated from the functional analysis effort are considered in the process, which should take into account the latest technology in the areas of design, producibility, and supportability. Synthesis requires input from all technology and engineering specialty areas that have a bearing on the system or design concept.	- Concept Design Sheet (CDS) - Schematic Block Diagrams (SBD) - Physical or mathematical models - Drawings, specifications, and other technical and supporting documentation.	DODI 5000.2, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*.

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
Evaluation and Decision (Trade Studies) This involves continual evaluation and decisions made throughout the design and development activity. Most attractive concepts are selected, evaluated, and optimized. Also, systems engineering identifies and documents the trade-off and supporting rationale and considers all possible solutions within the framework of requirements. (See also Section 3-11 and the Trade Studies/Trade-Off Analyses element, below, in this table.)	- Trade Study Report (TSR)	
Description of System Elements Once an acceptable solution or concept has been selected, interacting system elements are defined, which fall into five categories: 1) equipment/hardware, 2) software, 3) facilities, 4) personnel, and 5) procedural data. Performance, design, and test requirements for equipment end items, critical components, and computer software programs are established and described. Environmental requirements and interface design requirements imposed on facilities by the functional and design characteristics of equipment end items are identified and documented.	- Design Sheets - Facility Interface Sheets	DoD 4245.7-M, *Transition from Development to Production*.
Technical Performance Measurement/Performance Metrics (System Analysis and Control) Defined as the product design assessment that estimates, through engineering analysis and tests, the values of essential performance parameters of the current design of WBS product items. Used to forecast values to be achieved through the planned technical program effort; measure differences between the achieved values and those allocated to the product element by the systems engineering process; and determine the impact of these differences on system effectiveness. Purpose is to	- Contractor Technical Performance Measurement Report	*Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*; DI-S-3619, Technical Performance Measurement Report.

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
provide visibility of actual versus planned performance; provide early detection or prediction of problems that require management attention; and support assessment of the program impact of proposed change alternatives. Alerts program management to potential performance deficiencies before irrevocable cost or schedule impact occurs. Where risk management program is in place, provides data for technical risk planning and assessment. Can begin when configuration item requirements allocation is substantially complete (when draft Type B specifications are available, normally in the demonstration and validation phase). - Also, See Section 3.20, Metrics.		
Interface Management (System Analysis and Control) The documentation, management, and control of functional and performance interface requirements identified during functional analysis. Manages the interfaces within the system and between the system and the outside world; manages requirements as specified in interface control documents; systems engineering chairs Interface Control Working Group (ICWG). (See also Section 3.17)	- Interface Control Documents (ICD)	DODI 5000.2, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*; MIL-STD-973, *Configuration Management*; *NGCR Acquisition Guide (Draft)*.
System Integration The assurance, by systems engineering management, that all diverse elements of a system are compatible and ready when needed. Accomplished through proper planning and coordination through the development process. Basic plan for managing their effort is the Systems Engineering Management Plan (SEMP), prepared in three parts, by the contractor: Part I, "Technical Program Planning and Control", identifies organizational	- Contractor Systems Engineering Management Plan (SEMP)	

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
responsibilities and authority for systems engineering management, including control of subcontracted engineering, verification, configuration management, document management, and plans and schedules for design and technical program reviews; Part II, “Systems Engineering Process”, describes the process used in defining and allocating requirements and their documentation; Part III, Engineering Specialty Integration” defines how engineering specialties of reliability, maintainability, human factors engineering, safety, logistics support, and other areas are integrated into the mainstream design effort. SEMP provides the basis for all contractor system engineering efforts, should be program-specific, and should identify the organizational configuration, functions, and responsibilities, management techniques, analyses, trade studies, simulations, Technical Performance Measurement (TPM) parameters, and schedules that will be investigated and employed on the program.		

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
Risk Management (System Analysis and Control) Organized means of identifying and measuring risk (risk assessment) and developing, selecting, and managing options (risk analysis) for resolving or handling identified risks. Risk management strategy is established early in the program, and risk is continually addressed throughout the system life-cycle. Risk planning involves articulating program risk issues, identifying risk management strategy and techniques, defining project roles and responsibilities for risk management, developing risk identification, reporting, and tracking procedures. Risk identification involves soliciting risk insight from project personnel, performing risk identification as part of standing review boards, and employing experience from similar projects to identify potential risk. Risk analysis includes characterizing the types and magnitude of risks corresponding to the affected program baseline (technical, cost, schedule risk) and determining and evaluating the probability and impact of risk occurrence possibly through modeling techniques. Some aspects of risk handling include developing a risk avoidance strategy, such as selecting lower-risk technical approaches, choosing to control risk through management attention, transferring risk to another organization, performing research to understand risk sensitivities, and accepting risk as unavoidable. Once identified, risks are monitored and reevaluated until eliminated. Other techniques such as the WBS, TPM, CM, and trade-off analysis may also be considered risk management techniques used for risk assessment and management.	- Risk Management Templates - Contractor and Government Risk Management Plans (RMP) - Contractor Risk Sensitivity Analysis - Contractor Risk Handling Plans - Contractor Risk Reduction Reports - Schedule Network Models - Life-Cycle Cost Model	DODI 5000.2, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*; DoD 4245.7-2-M, *Transition from Development to Production*.

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
Trade Studies/Trade-Off Analysis (System Analysis and Control) Formal decision analysis method used to solve any complex problem where there is more than one selection criterion and to provide documented decision rationale. Necessary for establishing system configurations and for accomplishing detailed design of individual components. Applicable to budgeting, source selection, test planning, logistics development, production control, and design synthesis. (See also Section 3.11 and the Evaluation and Decision [Trade Studies] activity, above, in this table.)	- Trade-Off Analysis - Utility Curves - Weighted Summary Tables - Trade Study Reports (TSR)	DODI 5000.2, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*; DoD 4245.7-2-M, *Transition from Development to Production*; *NGCR Acquisition Guide (Draft)*.
Reliability Engineering Application of analytical methods and historical statistical data to determine equipment/system performance. Functional models of system performance are derived in accordance with the design, and a mathematical model with outputs of inherent failure distributions and failure rates. By analyzing the design and applying historical data, an estimate of the probability of successful performance (or failure) can be calculated for the system and for each segment, subsystem, assembly, and such. Reliability analysis identifies the strengths and weaknesses of the design, so that improvements can be made to the best advantage. Reliability estimates based on inherent (generic) failure rates are useful for planning purposes, for comparing alternatives, and for assessing proposed changes. Integration of this specialty is important during concept studies, trade-off analysis, design, and development.	- Failure Modes, Effects and Criticality Analysis (FMECA) - Sneak Circuit Analysis - Electronic Parts/Circuits Tolerance Analysis - Reliability Critical Items List - Effects of Functional Testing, Storage, Handling, Packaging, Transportation, and Maintenance - Environmental Stress Screening Report	MIL-STD-785, *Reliability Program for System and Equipment Development and Production*.

Systems Engineering Elements/Activities	Outputs/Product s	Governing Standards/Guidance
Maintainability Engineering Addresses the maintenance concept/policy as it is reflected in design provisions for fault prevention, detection, isolation and correction, and the implementation requirements in terms of skills, test equipment, time-to-repair/replace/restore, and maintenance cost over the life-cycle of the system or product. Maintenance concepts are based on operability considerations and on operations phase support concepts. Maintenance provisions are an important design factor in determining system availability and life-cycle cost. Maintainability program plan is normally submitted as part of the bidders' response to the RFP.	- Maintainability Program Plan	MIL-STD-470, *Maintainability Program Requirements for Systems and Equipment*.
Human Systems Integration Addresses people-equipment interfaces. Applies principles of human capability to reach, lift, see, communicate, comprehend, and act to the functions and circumstances required; allocates system functions to personnel, equipment, software, or facilities; identifies level of involvement and criticality of personnel tasks; and performs task analysis and timeline studies to determine if human capabilities will be exceeded. Specialists work with design, system safety, maintainability, testing, training, etc., personnel.	- Human Factors Planing documents and reports - Models and Mock-Ups	MIL-STD-46855, *Human Engineering Requirements for Military Systems, Equipment and Facilities*; MIL-STD-1472, *Human Engineering Design Criteria for Military Systems, Equipment and Facilities*; TAFIM Volume 8, *DoD Human Computer Interface (HCI) Style Guide*.

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
Specification Development Plays an integral role in the product development process and is the basic critical output of the systems engineering process. The system functional specification (Type A) and expanded lower-level specifications support a proposed technical solution to an approved operational requirement. Specifications applicable to C4I and information systems programs include the following types: **System/Segment (Type A)** states the technical and mission performance requirements for a system as an entity, allocates requirements to functional areas, documents design constraints, and defines interfaces between or among the functional areas. Based on parameters developed during the concept exploration and definition phase. **Development Specifications (Type B, Part I, Design-To)** state requirements for the design and engineering development of a product. Are applicable to an item below the system level and states performance and interface characteristics, and other technical detail sufficient to permit design, engineering for service use, and evaluation. Prepared typically late in the demonstration and validation phase. **Product Specifications (Type C)** are applicable to any level below the system level, and may be oriented toward procurement of a product through specification of primary functional (performance) requirements or primary production (detailed design) requirements. Contain complete performance requirements for intended use, interface and interchangeability characteristics (form, fit, function), detailed description of the product, performance requirements, and corresponding tests and inspections. Prepared in the later part of the development phase. (See also Section 3.14.3.1.)	- System/Segment (Type A) Specification - Development Specification (Type B) - Product Specification (Type C)	Report to SECDEF by USD(A), "Enhancing Defense Standardization-Specifications and Standards: Cornerstones of Quality", November 1988; MIL-STD-490A, *Specification Practices*; DoD 5000.43, *Acquisition Streamlining*; DoD-HDBK-248, *Guidance for Application and Tailoring of Requirements for Defense Material Acquisitions*; DEPSECDEF Memorandum of June 3, 1985, Acquisition Streamlining; DoDD 4120.3, *Defense Standardization and Specification Program*; DoD 4120.3-M, *Defense Standardization Manual*; DoD 4245.7-M, *Transition from Development to Production*.

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
System Safety Analysis of the system/program for hazards to personnel and equipment and the action taken to eliminate or control them. Encompasses all personnel and equipment that may be affected by program plans and operations. These include, but are not limited to, manufacturing, testing, packaging, handling, transportation, storage, and personnel and equipment at test and operational sites.	- Operational Hazard Analysis - Accidental Risk Assessment Report (ARAR)	MIL-STD-882, *System Safety Program Requirements*.
Configuration Management (CM) Integral part of the systems engineering management process for system definition and baseline management and control. Role is to: 1) identify the functional and physical characteristics of selected system components designated as configuration items; 2) control changes to those characteristics; 3) record and report change processing and implementation status; and 4) coordinate and support design reviews and configuration audits. Means through which the integrity and continuity of the design, engineering, and cost trade-off decisions made between technical performance, producibility, operability, testability, and supportability are recorded, communicated, and controlled by program and functional managers. At any given time, CM can supply current descriptions of developing and operational hardware and software configuration items and the system itself. Provides traceability to previous item and system baseline configurations and rationale for changes, thus permitting analysis and correction of deficiencies. Initiated as early as concept exploration and definition phase, by inputs from systems engineering, and continues throughout the system life-cycle. Provides for the identification and documentation of COTS/NDI, component compatibility, and	- Government and Contractor CM Plans - Configuration Status Accounting Reports - Functional, Allocated, and Product Baseline Listings - Configuration Audit Plans - Configuration Control Board (CCB) Agenda and Minutes	MIL-STD-973, *Configuration Management*; EIA/IS-649, *National Consensus Standard for Configuration Management*; ANSI/IEEE 1042-1987, *Guide to Software Configuration Management*; ANSI/IEEE 828-1990, *Software Configuration Management Plans*;

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
interface, and ensures that the functional characteristics of the system and system performance remain acceptable and documented. CM of COTS products should be done at the form, fit, function level, at the lowest organizational remove and replace level (i.e., LRU). Replacement products should be equivalent at the form, fit, function level. To ensure CM effectiveness, automated CM tools are required, especially for versioning source code and documentation, and the CM manager should report directly to the program manager.		
Technical Reviews (System Analysis and Control) Essential part of systems engineering process and means by which technical requirements and specifications are validated and configuration baselines are established. Can range from very formal technical reviews by Government and contractor systems engineers to very informal reviews involving few personnel and concerned with product and/or task elements of the WBS. Objective is to determine the technical adequacy of the existing design to meet known technical requirements. Reviews become more detailed and definitive as system moves through its life-cycle. The requirements and scheduling of formal reviews is normally included in the SOW of the contract and in the SEMP. They may include: System Requirements Review (SRR), System Design Review (SDR), Preliminary Design Review (PDR), Software Specification Review (SSR), Critical Design Review (CDR), Test Readiness Review (TRR), Functional Qualification Review (FQR), and Production Readiness Review (PRR).	- Technical Review Agenda and Minutes (Contractor) - Contractor's Technical Review Data Package (Contractor	MIL-STD-973, *Configuration Management*; DoDI 5000.38, *Production Readiness Reviews*.

Systems Engineering Elements/Activities	Outputs/Products	Governing Standards/Guidance
The requirements and need for review is controlled by DODI 5000.2, Part 4, "Program Design" , and MIL-STD-973, which should be tailored to factors such as program complexity, level of inherent technical risk, and number of participating contractors.		
Test and Evaluation (T&E) See Section 3.18 for the description of T&E.	See Section 3.18.	DoDD 5000. 1 *Defense Acquisition*; *NGCR Acquisition Guide (Draft)*.
Integrated Logistics Support (ILS) See Section 3.19 for the description of ILS.	See Section 3.19	DoDD 5000.1 *Defense Acquisition*;
Producibility N/A - Engineering function directed toward achieving a design compatible with the realities of available manufacturing processes and not considered applicable to C4I and information systems.	N/A	N/A
Life-Cycle Cost Analysis Structured study of life-cycle cost (LCC) estimates and elements to identify life-cycle cost drivers, total cost to the Government, cost risk items, and cost-effective changes. It is a systems engineering tool with application to all elements of the system. Computer modeling is often used to identify and analyze cost drivers, which are areas where resources can best be applied to achieve the greatest benefit in reduced cost. Modeling for LCC is also useful in cost-benefit and cost-effectiveness studies, long-range planning, and budgeting, comparison of competing systems, decisions about replacement of aging equipment, control of an ongoing program, and selection among competing contractors.	- Life-Cycle Cost Reports	OMB Circular A-76, Supplement 1, Cost Comparison Handbook; DoD 4245, *Design to Cost*; AFR 800-11, Life-Cycle Costing.

This page intentionally left blank.

APPENDIX F

OSE INFORMATION SERVICES

F.1 The following table contains a listing of DISA services available for obtaining additional OSE guidance and information pertaining to the TAFIM and related OSE requirements.

- To Be Provided -

This page intentionally left blank.

APPENDIX G

PROGRAM MANAGEMENT RESPONSIBILITIES MATRIX

G.1 The following table identifies the program management areas discussed in Volume 5, the documentation to be produced in relation to each area, and the DoD management level(s) responsible for the products identified.

- To Be Provided -

This page intentionally left blank.

APPENDIX H

PROPOSING CHANGES TO TAFIM VOLUMES

H.1 INTRODUCTION

Changes to the TAFIM will occur through changes to the TAFIM documents (i.e., the TAFIM numbered volumes, the CMP, and the PMP). This appendix provides guidance for submitting proposed TAFIM changes. These proposals should be described as specific wording for line-in/line-out changes to a specific part of a TAFIM document.

Use of a standard format for submitting a change proposal will expedite the processing of changes. The format for submitting change proposals is shown in Section H.2. Guidance on the use of the format is provided in Section H.3.

A Configuration Management contractor is managing the receipt and processing of TAFIM change proposals. The preferred method of proposal receipt is via e-mail in ASCII format, sent via the Internet. If not e-mailed, the proposed change, in the format shown in Section H.2, and provide on both paper and floppy disk, should be mailed. As a final option, change proposals may be sent via fax; however, delivery methods that enable electronic capture of change proposals are preferred. Address information for the Configuration Management contractor is shown below.

Internet: **tafim@bah.com**

Mail: **TAFIM**

Booz•Allen & Hamilton Inc.

5201 Leesburg Pike, 4th Floor

Falls Church, VA 22041

Fax: **703/671-7937**; indicate "TAFIM" on cover sheet.

H.2 TAFIM CHANGE PROPOSAL SUBMISSION FORMAT

a. Point of Contact Identification

(1) Name:

(2) Organization and Office Symbol:

(3) Street:

(4) City:

(5) State:

(6) Zip Code:

(7) Area Code and Telephone #:

(8) Area Code and Fax #:

(9) E-mail Address:

b. Document Identification

(1) Volume Number:

(2) Document Title:

(3) Version Number:

(4) Version Date:

c. Proposed Change # 1

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

d. Proposed Change # 2

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

n. Proposed Change # n

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

H.3 FORMAT GUIDANCE

The format in Section H.2 should be followed exactly as shown. For example, Page Number should not be entered on the same line as the Section Number. The format can accommodate, for a specific TAFIM document, multiple change proposals for which the same individual is the Point of Contact (POC). This POC would be the individual the TAFIM project staff could contact with any questions regarding the proposed change. The information in the **Point of Contact Identification** Part (**H.2a**) would identify that individual. The information in the **Document Identification** (**H.2b**) is self-evident, except that a volume number would not apply to the CMP or PMP. The proposed changes would be described in the **Proposed Change #** (**H.2c, H.2d, or H.2n**).

In the **Proposed Change #** parts of the format, the Section Number refers to the specific subsection of the document in which the change is to take place (e.g., Section 2.2.3.1). The page number (or numbers, if more than one page is involved) will further identify where in the document the proposed change is to be made. The Title of Proposed Change field is for the submitter to insert a brief title that gives a general indication of the nature of the proposed change. In the Wording of Proposed Change field the submitter will identify the specific words (or sentences) to be deleted and the exact words (or sentences) to be inserted; providing identification of the referenced paragraph, as well as the affected sentence(s) in that paragraph, would be helpful. An example of input for this field would be: “Delete the last sentence of the second paragraph of the section and replace it with the following sentence: “The working baseline will only be available to the TAFIM project staff.” The goal is for the submitter to provide proposed wording that is appropriate for insertion into a TAFIM document without editing (i.e., a line-out/line-in change). The H.2c (5), H.2d (5), or H.2n (5) entry in this part of the format is a discussion of the rationale for the change. The rationale may include reference material. Statements such as “industry practice” would carry less weight than specific examples. In addition, to the extent possible, submitters should provide citations from professional publications. A statement of the impact of the proposed change may also be included with the rationale. Finally, any other information related to the improvement of the specific TAFIM document may be provided in H.2 c (6), H.2 d (6), or H.2 n (6) (i.e., the Other Comments field). However, without some degree of specificity these comments may not result in change to the document.

This page intentionally left blank.

APPENDIX J

INFORMATION SYSTEM ARCHITECTURE RELATIONSHIPS AND DEFINITIONS

J.1 This appendix has been created to include the definitions being developed by DISA/D5 in the *Information System Architecture Relationships and Definitions* draft document. This document is being staffed separately. This coordinated version will be incorporated in this appendix in the Version 3.0 Final.

-To Be Provided-

This page intentionally left blank.